PHILIPS

Security Testing Report

SWPIC

EIPF_1.1.0

Table of Contents

Document Version Control

Name of the document : EIPF 1.1.0 Security Testing Report			
Version: 1.0	**Intake ID:**	2844	
Document Definition: This document highlights the vulnerabilities currently existing in the application under scope. It also documents possible actions to be taken to reduce/eliminate the vulnerabilities.	**Document ID:**	PRHC/C40/SVN/88998	
Author: Sai Praneetha Bhaskaruni, Navin Kumar Pari	**Effective Date:**	28/Nov/2023	
Reviewed by: Shabana Bagum			

Document History

Version	Date	Author	Section	Changes
0.1	27 Nov 2023	Sai Praneetha Bhaskaruni, Navin Kumar Pari	Complete	Initial Draft
1.0	28 Nov 2023	Shabana Bagum	Complete	Final Review

Distribution List

User/Department/Stakeholder	E-Mail ID
Project Owner and PSO	amber.lee@philips.com; Frank.LIU@philips.com; Terry.YANG@philips.com; fan.yu@philips.com; juanjuan.duan@philips.com

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

1. Definitions & Abbreviations

Term	**Explanation**
SCoE	Security Center of Excellence
TLS	Transport Layer Security
SSL	Secure Socket Layer
XSS	Cross Site Scripting

The severity of every vulnerability has been calculated by using industry standard **Common Vulnerability Scoring System (CVSS)** used for assessing the severity of computer system vulnerabilities. CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score (Scores range from 0 to 10, with 10 being the most severe) reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organization properly assess and prioritize their vulnerability management processes.

The severity rating for the numerical values are mapped below

None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

The **Severity** and **CVSS vector** of each vulnerability is calculated using the CVSS V3 **Base Score Metrics** Calculator located here. Vulnerabilities identified during security assessment are classified into standardized categories. Refer following table for more information:

Categories for vulnerability classification

Web application security assessment	OWASP Top Ten - 2021
Mobile application security assessment	OWASP Top Ten - 2016
IoT/Hardware security assessment	OWASP Top Ten - 2014

2. System Details & Architecture

Brief about the system:

There are different services in EIPF such as adding/retreiving/update/Delete Dictionary mappings and other services related to Reports.

There were windows services such as

HSC.EIPF.DomainMappingSyncService.exe
HSC.EIPF.FhirSyncService.exe
HSC.EIPF.NotificationService.exe

Environment: gateway

Version- 1.1.0

3. Scope

The scope of this security assessment is to perform **Grey-Box** security testing to find security threats that may come from a malicious outsider or insider user of the **EIPF_1.1.0**. Security testing on **Web services & windows service** of the **EIPF_1.1.0** is performed.

The following list includes few examples of major activities performed during this assessment:

Web Application/Web Services:

- Crawl through complete scope of the web application/service space and identify for any unauthenticated URL or directory.
- Check for all input injection-based attacks across all the possible entry fields in Web API.
- Exploiting any known component vulnerability or service misconfiguration.
- Reviewing the transport layer security implemented.

Windows Services:

- Exploiting any known component vulnerability or service misconfiguration.
- Services are checked for local storage.
- Check for Permissions.

Follow "Test case execution" section for detailed test cases.

Start Date	End Date	Applications/Devices/IP's/URL's
20/Nov/2023	22/Nov/2023	Webservices/API's: { } EIPF Ptest 1.1.0.postman_collecti
23/Nov/2022	24/Nov/2022	Windows Services: • HSC.EIPF.DomainMappingSyncService.exe • HSC.EIPF.FhirSyncService.exe • HSC.EIPF.NotificationService.exe

Not In Scope

Below Mentioned items are out of scope for the current security assessment:

- Source code review
- Network & Infrastructure security assessment
- Complete Thick client assessment

- All other APIs.

4. Executive Summary

Security Center of Excellence (SCoE) team is engaged in activities to conduct security assessment of **EIPF_1.1.0** which included **web services & windows services** in scope. The purpose of the engagement is to evaluate the security of the **EIPF_1.1.0** against industry best practice criteria.

Note: Only highlights of important vulnerabilities are described below. Please refer 'Vulnerability Summary' section for complete detailed list of vulnerabilities.

During the security assessment following factors are found with consideration for significant improvement:

- JWT Misconfiguration
- SQL Injection

During the security assessment of web application, security issues in the below areas are not found:

- Privilege escalation

VULNERABILITY SUMMARY TABLE

The table below shows a summary of the number of vulnerabilities and their severities.

Note: The vulnerabilities mentioned in this report are technical vulnerabilities only. The Product Security Risk Assessment would report the business risks associated with these vulnerabilities.

Critical	High	Medium	Low
0	1	2	10

5. Vulnerability Summary

The Findings and vulnerabilities from the assessment are tabulated below

Finding No.	Vulnerability Title	Severity	Impacted Area	CVE ID*	Status
89290	SQL Injection	High	Webservices	NA	Open
89293	JWT Misconfiguration	Medium	Webservices	NA	Open
89287	Insecure CORS	Low	Webservices	NA	Open
89291	Delete method is enabled	Low	Webservices	NA	Open
89289	Lack of Input Validation	Low	Webservices	NA	Open
89292	Weak SSL/TLS Configuration	Low	Webservices	NA	Open
89286	Verbose Server Banner	Low	Webservices	NA	Open
89288	Improper Error Handling	Low	Webservices	NA	Open
89345	Sensitive Data in Memory	Medium	WindowsServices	NA	Open
89365	Unsigned Binaries	Low	WindowsServices	NA	Open
89368	PDB files included in the Binary	Low	WindowsServices	NA	Open
89344	DLL Injection	Low	WindowsServices	NA	Open
89369	Insecure Windows Service Permissions	Low	WindowsServices	NA	Open

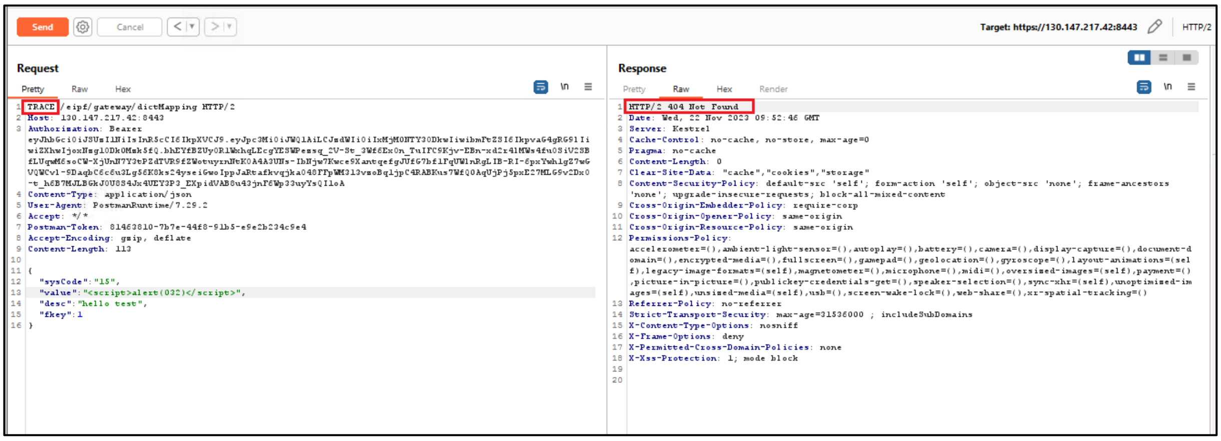
*CVE ID are mentioned for the vulnerabilities which has a known external CVE.

6. Observations

Below mentioned observations are not considered as Vulnerability but informative to the business.

Observations which shows good implementation or best practice identified:

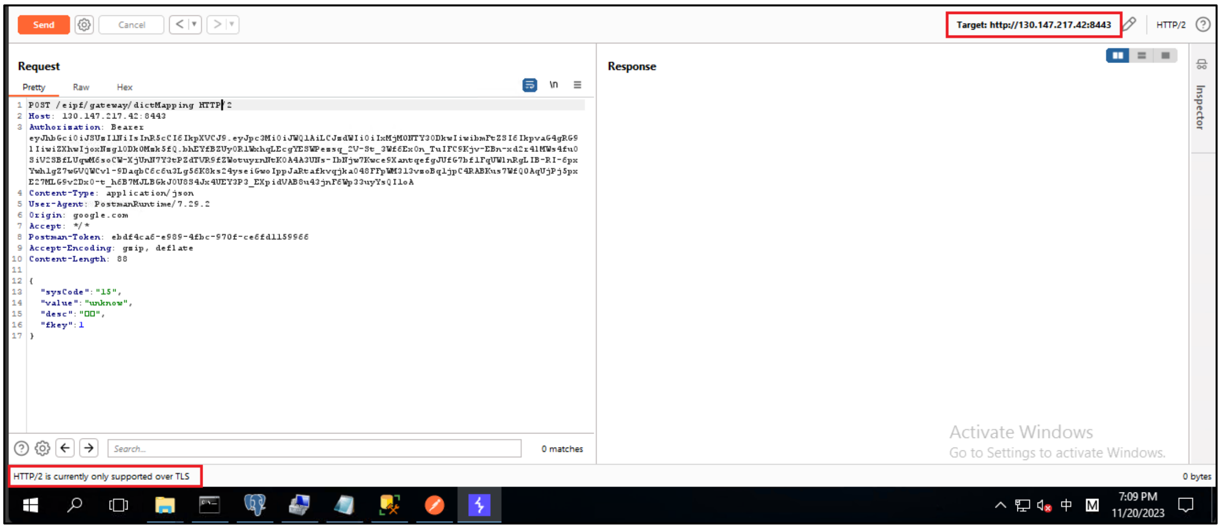
- It is observed that the endpoint is not allowing Trace method.



```
TRACE /eipf/gateway/dictMapping HTTP/2
Host: 130.147.217.42:8443
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJWQ1AiLCJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIi
wiZXhwIjoxNzg1ODk0Mzk5fQ.bhEYfBZUy0R1WxhqLEcgYESWPezsq_2V-St_3Wf6Ex0n_TuIFC9Kjv-EBn-xd2r41MWs4fu0SiV2SB
fLUqwM6soCW-XjUnN7Y3tPZdTVR9fZWotuyrnNtK0A4A3UNs-IbNjw7Kwce9XantqefgJUfG7bf1FqUWlnRgLIB-RI-6pxYwh1gZ7wG
VQWCvl-9DaqbC6c6u3Lg56K8ks24yseiGwoIppJaRtafkvqjka048FFpWM313vzoBq1jpC4RABKus7WfQ0AqUjPj5pxE27MLG9v2Dx0
-t_h6B7MJLBGkJ0U8S4Jx4UEY3P3_EXpidVAB8u43jnF6Wp33uyYsQIloA
Content-Type: application/json
User-Agent: PostmanRuntime/7.29.2
Accept: */*
Postman-Token: 81463810-7b7e-44f8-91b5-e9e2b234c9e4
Accept-Encoding: gzip, deflate
Content-Length: 113

{
  "sysCode":"15",
  "value":"<script>alert(032)</script>",
  "desc":"hello test",
  "fkey":1
}
```

```
HTTP/2 404 Not Found
Date: Wed, 22 Nov 2023 09:52:46 GMT
Server: Kestrel
Cache-Control: no-cache, no-store, max-age=0
Pragma: no-cache
Content-Length: 0
Clear-Site-Data: "cache","cookies","storage"
Content-Security-Policy: default-src 'self'; form-action 'self'; object-src 'none'; frame-ancestors
'none'; upgrade-insecure-requests; block-all-mixed-content
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Permissions-Policy:
accelerometer=(),ambient-light-sensor=(),autoplay=(),battery=(),camera=(),display-capture=(),document-d
omain=(),encrypted-media=(),fullscreen=(),gamepad=(),geolocation=(),gyroscope=(),layout-animations=(sel
f),legacy-image-formats=(self),magnetometer=(),microphone=(),midi=(),oversized-images=(self),payment=()
,picture-in-picture=(),publickey-credentials-get=(),speaker-selection=(),sync-xhr=(self),unoptimized-im
ages=(self),unsized-media=(self),usb=(),screen-wake-lock=(),web-share=(),xr-spatial-tracking=()
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Content-Type-Options: nosniff
X-Frame-Options: deny
X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 1; mode block
```

- Endpoint is not accessible over HTTP.



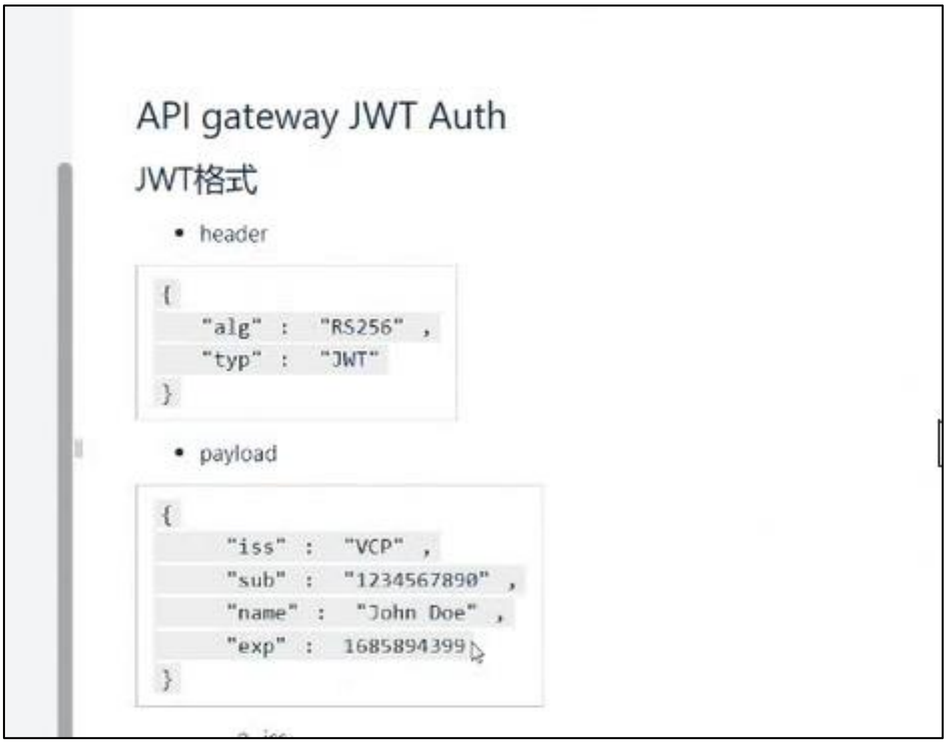
Target: http://130.147.217.42:8443

```
POST /eipf/gateway/dictMapping HTTP/2
Host: 130.147.217.42:8443
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJWQ1AiLCJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9
lIiwiZXhwIjoxNzg1ODk0Mzk5fQ.bhEYfBZUy0R1WxhqLEcgYESWPezsq_2V-St_3Wf6Ex0n_TuIFC9Kjv-EBn-xd2r41MWs4fu0
SiV2SBfLUqwM6soCW-XjUnN7Y3tPZdTVR9fZWotuyrnNtK0A4A3UNs-IbNjw7Kwce9XantqefgJUfG7bf1FqUWlnRgLIB-RI-6px
Ywh1gZ7wGVQWCvl-9DaqbC6c6u3Lg56K8ks24yseiGwoIppJaRtafkvqjka048FFpWM313vzoBq1jpC4RABKus7WfQ0AqUjPj5px
E27MLG9v2Dx0-t_h6B7MJLBGkJ0U8S4Jx4UEY3P3_EXpidVAB8u43jnF6Wp33uyYsQIloA
Content-Type: application/json
User-Agent: PostmanRuntime/7.29.2
Origin: google.com
Accept: */*
Postman-Token: ebdf4ca6-e989-4fbc-970f-ce6fd1159966
Accept-Encoding: gzip, deflate
Content-Length: 88

{
  "sysCode":"15",
  "value":"unknow",
  "desc":"□□",
  "fkey":1
}
```

HTTP/2 is currently only supported over TLS

Observations which shows weak implementation:

- Generating the JWT token from https://jwt.io/ using the below information(test data) is not a good practice.



API gateway JWT Auth

JWT格式

- header

```
{
    "alg"  :  "RS256"  ,
    "typ"  :  "JWT"
}
```

- payload

```
{
      "iss"  :  "VCP"  ,
      "sub"  :  "1234567890"  ,
      "name"  :  "John Doe"  ,
      "exp"  :  1685894399
}
```

7. Detailed Vulnerability Report

7.1 WebServices: SQL Injection

Vulnerability Title	SQL Injection
Vulnerability Category	A3 Injection
Severity	**High**
CVSS V3 Calculation	CVSS Base Score: 9.0 CVSS:3.1/ AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
Description	**Vulnerability Description:** During the assessment, it is observed that when we Input the payload WAIT FOR DELAY ‘0:0:5’ -- the response got delayed by 5 seconds. SQL Injection (SQLi) is an injection attack wherein an attacker can execute malicious SQL statements bypassing the validation, that when executed can control a web application’s database server. **Reference:** https://owasp.org/www-community/attacks/SQL_Injection **Exploitability rational:** An attacker should have access to API to manipulate the input fields which interacts with the sql query. **Impact rational:** A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete) thereby affecting data integrity, execute administration operations on the database, recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. An attacker can use it to bypass a web application’s authentication and authorization mechanisms and retrieve the contents of an entire database.
Affected Systems/IP Address/URL	https://130.147.217.42:8443/eipf/gateway/deletePrivacyData

Recommendation	• Rewrite all SQL queries constructed through dynamic concatenation to use an injection-safe query mechanism such as prepared statements with parameterized queries. • Stored Procedure can be used to mitigate SQL Injection • Rather than construct the dynamic SQL query by concatenating user-supplied data to static SQL query string fragments, data values are identified in the query by parameter markers or variables. Dynamic data is then passed through a mechanism provided by SQL that prevents the supplied data from changing the meaning of the query. • Input Validation can be considered as a defense as well. **Reference:** https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html Note: The exact syntax and use of prepared statements with parameterized queries varies from language to language. The following links provide general guidance for secure SQL query construction in .NET, Java, and PHP: • https://msdn.microsoft.com/en-us/library/bb738521(v=vs.100).aspx • https://docs.oracle.com/javase/tutorial/jdbc/basics/prepared.html • http://php.net/manual/en/mysqli.prepare.php
Status	**Open**

Steps to Reproduce

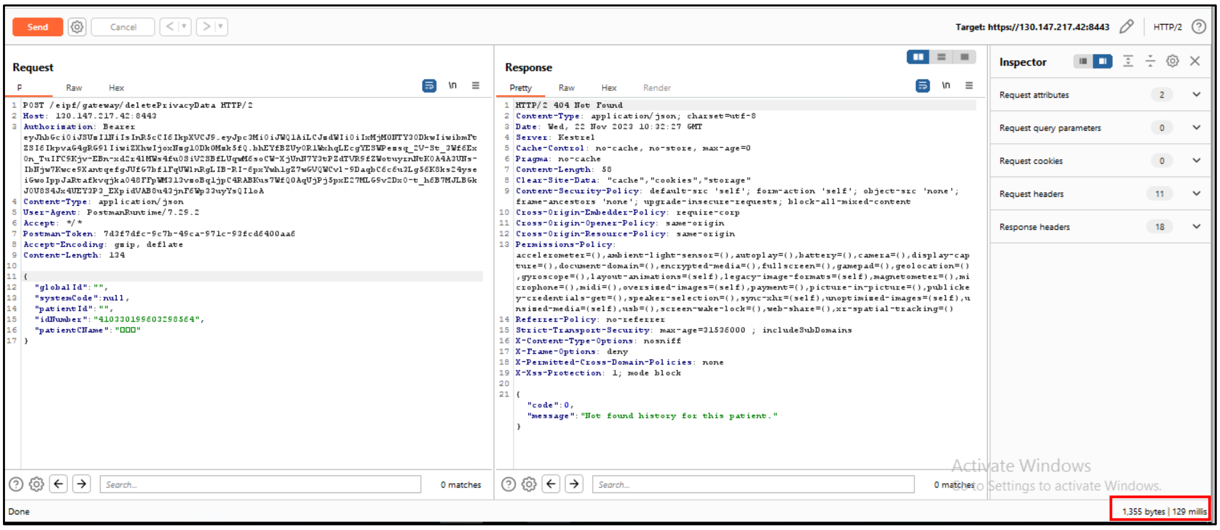
Step 1: Configure the browser to use poxy tool such as Burp Suite.

Step 2: Log into the application.

Step 3: Navigate to https://130.147.217.42:8443/eipf/gateway/deletePrivacyData.

Step 4: Input the payload(e.g. ‘;WAIT FOR DELAY ‘0:0:5’ --) and observe that the response got delayed by 5 seconds thereby confirming SQL injection in the application as shown in the screenshot below:

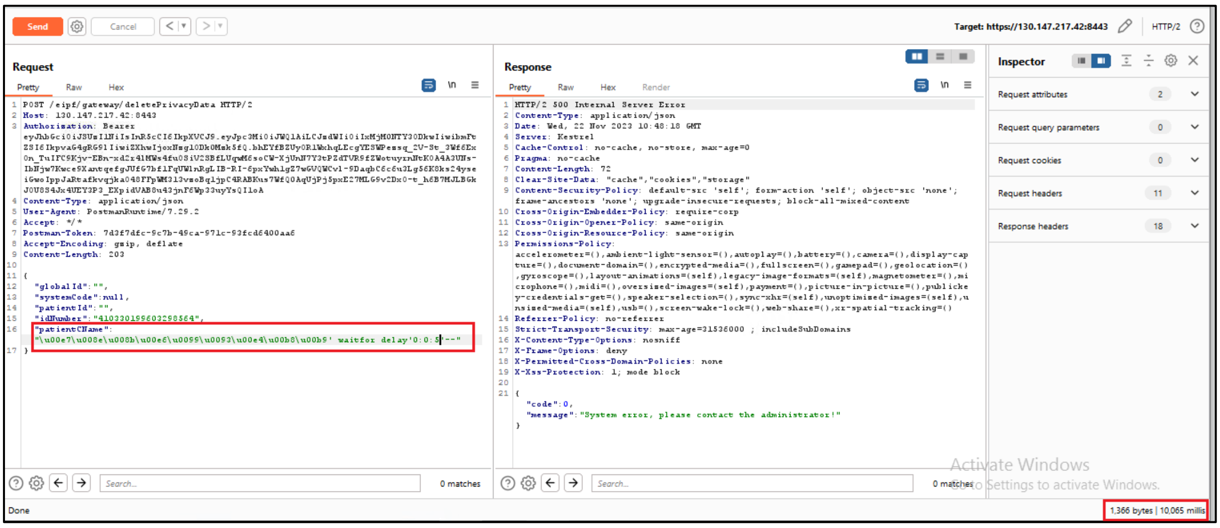
Supportive Evidence:



```
POST /eipf/gateway/deletePrivacyData HTTP/2
Host: 130.147.217.42:8443
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJWQ1AiLCJzdWIiOiIxMjM0NTY3ODkwIiwibmFt
ZSI6IkpvaG4gRG9lIiwiZXhwIjoxNzg1ODk0Mzk5fQ.bhEYfBZUy0R1WxhqLEcgYESWPessq_2V-St_3Wf6Ex
0n_TuIFC9Kjv-EBn-xd2r41MWs4fu0SiV2SBfLUqwM6soCW-XjUnN7Y3tPZdTVR9fZWotuyrnNtK0A4A3UNs-
IbNjw7Kwce9XantqefgJUfG7bf1FqUWlnRgLIB-RI-6pxYwh1gZ7wGVQWCvl-9DaqbC6c6u3Lg56K8ks24yse
iGwoIppJaRtafkvqjka048FFpWM313vzoBq1jpC4RABKus7WfQ0AqUjPj5pxE27MLG9v2Dx0-t_h6B7MJLBGk
J0U8S4Jx4UEY3P3_EXpidVAB8u43jnF6Wp33uyYsQIloA
Content-Type: application/json
User-Agent: PostmanRuntime/7.29.2
Accept: */*
Postman-Token: 7d3f7dfc-9c7b-49ca-971c-93fcd6400aa6
Accept-Encoding: gzip, deflate
Content-Length: 134

{
  "globalId":"",
  "systemCode":null,
  "patientId":"",
  "idNumber":"410330199603298564",
  "patientCName":"□□□"
}
```

```
HTTP/2 404 Not Found
Content-Type: application/json; charset=utf-8
Date: Wed, 22 Nov 2023 10:32:27 GMT
Server: Kestrel
Cache-Control: no-cache, no-store, max-age=0
Pragma: no-cache
Content-Length: 58
Clear-Site-Data: "cache","cookies","storage"
Content-Security-Policy: default-src 'self'; form-action 'self'; object-src 'none';
frame-ancestors 'none'; upgrade-insecure-requests; block-all-mixed-content
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Permissions-Policy:
accelerometer=(),ambient-light-sensor=(),autoplay=(),battery=(),camera=(),display-cap
ture=(),document-domain=(),encrypted-media=(),fullscreen=(),gamepad=(),geolocation=()
,gyroscope=(),layout-animations=(self),legacy-image-formats=(self),magnetometer=(),mi
crophone=(),midi=(),oversized-images=(self),payment=(),picture-in-picture=(),publicke
y-credentials-get=(),speaker-selection=(),sync-xhr=(self),unoptimized-images=(self),u
nsized-media=(self),usb=(),screen-wake-lock=(),web-share=(),xr-spatial-tracking=()
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Content-Type-Options: nosniff
X-Frame-Options: deny
X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 1; mode block

{
  "code":0,
  "message":"Not found history for this patient."
}
```

Original Request



```
POST /eipf/gateway/deletePrivacyData HTTP/2
Host: 130.147.217.42:8443
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJWQ1AiLCJzdWIiOiIxMjM0NTY3ODkwIiwibmFt
ZSI6IkpvaG4gRG9lIiwiZXhwIjoxNzg1ODk0Mzk5fQ.bhEYfBZUy0R1WxhqLEcgYESWPessq_2V-St_3Wf6Ex
0n_TuIFC9Kjv-EBn-xd2r41MWs4fu0SiV2SBfLUqwM6soCW-XjUnN7Y3tPZdTVR9fZWotuyrnNtK0A4A3UNs-
IbNjw7Kwce9XantqefgJUfG7bf1FqUWlnRgLIB-RI-6pxYwh1gZ7wGVQWCvl-9DaqbC6c6u3Lg56K8ks24yse
iGwoIppJaRtafkvqjka048FFpWM313vzoBq1jpC4RABKus7WfQ0AqUjPj5pxE27MLG9v2Dx0-t_h6B7MJLBGk
J0U8S4Jx4UEY3P3_EXpidVAB8u43jnF6Wp33uyYsQIloA
Content-Type: application/json
User-Agent: PostmanRuntime/7.29.2
Accept: */*
Postman-Token: 7d3f7dfc-9c7b-49ca-971c-93fcd6400aa6
Accept-Encoding: gzip, deflate
Content-Length: 203

{
  "globalId":"",
  "systemCode":null,
  "patientId":"",
  "idNumber":"410330199603298564",
  "patientCName":
  "\u00e7\u008e\u008b\u00e6\u0099\u0093\u00e4\u00b8\u00b9' waitfor delay'0:0:5'--"
}
```

```
HTTP/2 500 Internal Server Error
Content-Type: application/json
Date: Wed, 22 Nov 2023 10:48:18 GMT
Server: Kestrel
Cache-Control: no-cache, no-store, max-age=0
Pragma: no-cache
Content-Length: 72
Clear-Site-Data: "cache","cookies","storage"
Content-Security-Policy: default-src 'self'; form-action 'self'; object-src 'none';
frame-ancestors 'none'; upgrade-insecure-requests; block-all-mixed-content
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Permissions-Policy:
accelerometer=(),ambient-light-sensor=(),autoplay=(),battery=(),camera=(),display-cap
ture=(),document-domain=(),encrypted-media=(),fullscreen=(),gamepad=(),geolocation=()
,gyroscope=(),layout-animations=(self),legacy-image-formats=(self),magnetometer=(),mi
crophone=(),midi=(),oversized-images=(self),payment=(),picture-in-picture=(),publicke
y-credentials-get=(),speaker-selection=(),sync-xhr=(self),unoptimized-images=(self),u
nsized-media=(self),usb=(),screen-wake-lock=(),web-share=(),xr-spatial-tracking=()
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Content-Type-Options: nosniff
X-Frame-Options: deny
X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 1; mode block

{
  "code":0,
  "message":"System error, please contact the administrator!"
}
```

7.2 WebServices: JWT Misconfiguration

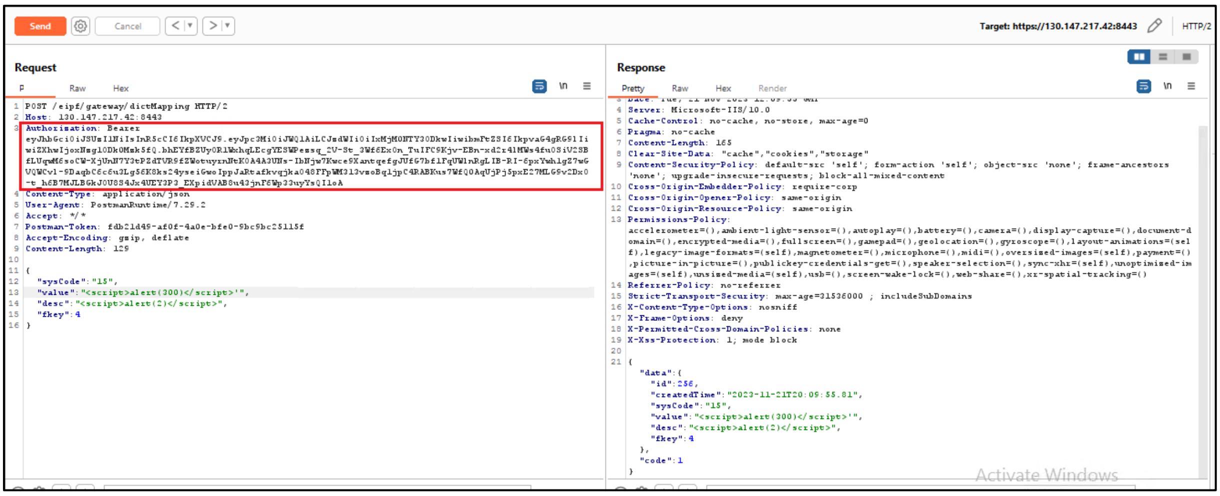
Vulnerability Title	JWT Misconfiguration
Vulnerability Category	A5 Security Misconfiguration
Severity	**Medium**
CVSS V3 Calculation	CVSS Base Score: 5.9 CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
Description	**Vulnerability Description:** During the assessment, it is observed that the APIs used to communicate to the servers are validated by the JWT auth token which has no expiry and same token as being used. JWT is an open standard (RFC 7519) for defining JSON objects shared between multiple systems and representing a user's identity or specific permission associated with that identity. JWT tokens are commonly used in authentication and authorization processes to prove a user's identity or grant access to specific protected resources or actions. **Reference:** 2020-01_Attacking_and_Securing_JWT.pdf (owasp.org) **Exploitability Rational:** To exploit the vulnerability, an attacker should have network access to the server via HTTP channel. **Impact Rational:** If the token never gets expired, if the token is stolen by an attacker then the attacker can always access the user's data.
Affected Systems/IP Address/URL	EIPF Ptest 1.1.0.postman_collection.json.zip
Recommendation	It is recommended to set JWT expiration. **Reference:** JSON Web Token for Java - OWASP Cheat Sheet Series
Status	**Open**

Steps to Reproduce

Step 1: Configure postman to work with a proxy tool such as Burp suite.

Step 2: Intercept the request and send to Repeater. Observe that the JWT token can be reused or it does not have any expiry time.

Supportive Evidence:



```
POST /eipf/gateway/dictMapping HTTP/2
Host: 130.147.217.42:8443
Authorisation: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJWQ1AiLCJsdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiZXhwIjoxNzg1ODk0Mzk5fQ.bhEYfBZUy0R1WxhqLEcgYESWPessq_2V-St_3Wf6Ex0n_TuIFC9Kjv-EBn-xd2r41MWs4fu0SiV2SBfLUqwM6soCW-XjUnN7Y3tPZdTVR9fZWotuyrnNtK0A4A3UNs-IbNjw7Kwce9XantqefgJUfG7bf1FqUWlnRgLIB-RI-6pxYwhlgZ7wGVQWCvl-9DaqbC6c6u3Lg56K8ks24yseiGwoIppJaRtafkvqjka048FFpWM313vsoBq1jpC4RABKus7WfQ0AqUjPj5pxE27MLG9v2Dx0-t_h6B7MJLBGkJ0U8S4Jx4UEY3P3_EXpidVAB8u43jnF6Wp33uyYsQIloA
Content-Type: application/json
User-Agent: PostmanRuntime/7.29.2
Accept: */*
Postman-Token: fdb21d49-af0f-4a0e-bfe0-9bc9bc25115f
Accept-Encoding: gzip, deflate
Content-Length: 129

{
  "sysCode":"15",
  "value":"<script>alert(300)</script>'",
  "desc":"<script>alert(2)</script>",
  "fkey":4
}
```

```
Date: Tue, 21 Nov 2023 12:09:55 GMT
Server: Microsoft-IIS/10.0
Cache-Control: no-cache, no-store, max-age=0
Pragma: no-cache
Content-Length: 165
Clear-Site-Data: "cache","cookies","storage"
Content-Security-Policy: default-src 'self'; form-action 'self'; object-src 'none'; frame-ancestors
'none'; upgrade-insecure-requests; block-all-mixed-content
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Permissions-Policy:
accelerometer=(),ambient-light-sensor=(),autoplay=(),battery=(),camera=(),display-capture=(),document-d
omain=(),encrypted-media=(),fullscreen=(),gamepad=(),geolocation=(),gyroscope=(),layout-animations=(sel
f),legacy-image-formats=(self),magnetometer=(),microphone=(),midi=(),oversized-images=(self),payment=()
,picture-in-picture=(),publickey-credentials-get=(),speaker-selection=(),sync-xhr=(self),unoptimized-im
ages=(self),unsized-media=(self),usb=(),screen-wake-lock=(),web-share=(),xr-spatial-tracking=()
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Content-Type-Options: nosniff
X-Frame-Options: deny
X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 1; mode block

{
  "data":{
    "id":256,
    "createdTime":"2023-11-21T20:09:55.81",
    "sysCode":"15",
    "value":"<script>alert(300)</script>'",
    "desc":"<script>alert(2)</script>",
    "fkey":4
  },
  "code":1
}
```

7.3 WebServices: Insecure CORS

Vulnerability Title	Insecure CORS
Vulnerability Category	A5 Security Misconfiguration
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.4 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N
Description	**Vulnerability Description:** During the assessment, it is observed that the server has responded to the request with headers 'Access-Control-Allow-Origin' which is set to wildcard. Cross-origin resource sharing (CORS) is a browser mechanism which enables controlled access to resources located outside of a given domain. It extends and adds flexibility to the same-origin policy (SOP). An insecure CORS configuration allows any website to trigger requests with user credentials to the target application and read the responses, thus enabling attackers to perform privileged actions or to retrieve potential sensitive information. References: • https://owasp.org/www-community/attacks/CORS_OriginHeaderScrutiny • https://www.tenable.com/plugins/was/98983 • https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS **Exploitability rational:** Malicious websites are able to access and take advantage of the web server's API endpoints due to poor CORS header setting. **Impact rational:** An attacker can access sensitive data of victim. An unrestricted CORS policy allows an attacker to access sensitive data or perform unauthorized user actions without user knowledge.

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.

Affected Systems/IP Address/URL	https://130.147.217.42:8443/eipf/gateway/dictMapping
Recommendation	The Access-Control-Allow-Origin header should not be set to a wildcard match. In most cases, this header can be safely removed. However, if the application requires a relaxation of the Same Origin Policy, the Access-Control-Allow-Origin header should whitelist only domains that are trusted by this server. Reference: https://cheatsheetseries.owasp.org/cheatsheets/HTML5_Security_Cheat_Sheet.html#cross-origin-resource-sharing
Status	**Open**

Steps to Reproduce

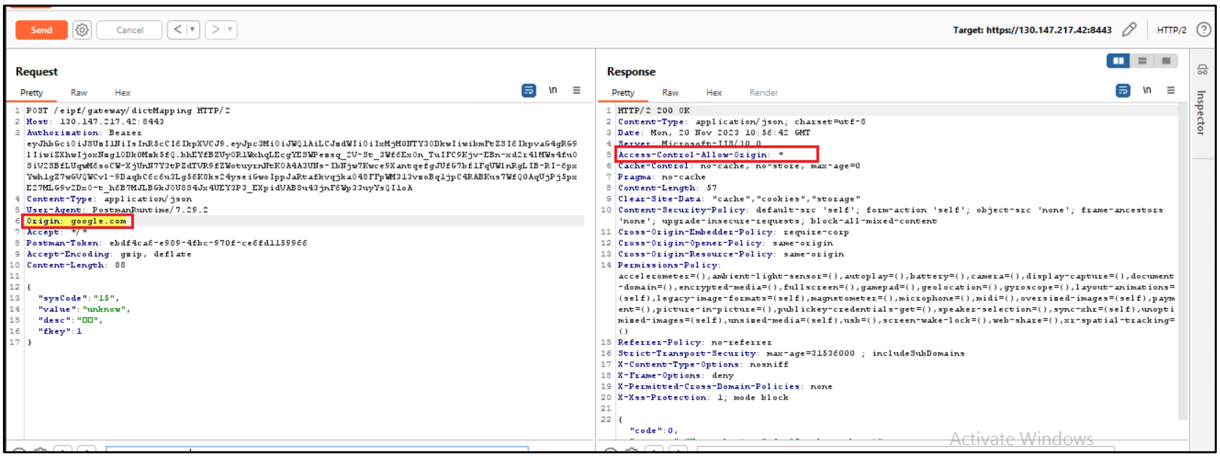
Step 1: Login to the application and intercept the application traffic using web proxy tools like Burp suite.

Step 2: Send the captured request to the repeater tab.

Step 3: Change the value of the origin header and forward the request to server.

Step 4: Observe that the server has responded to the request with headers 'Access-Control-Allow-Origin' set to wildcard.

Supportive Evidence:



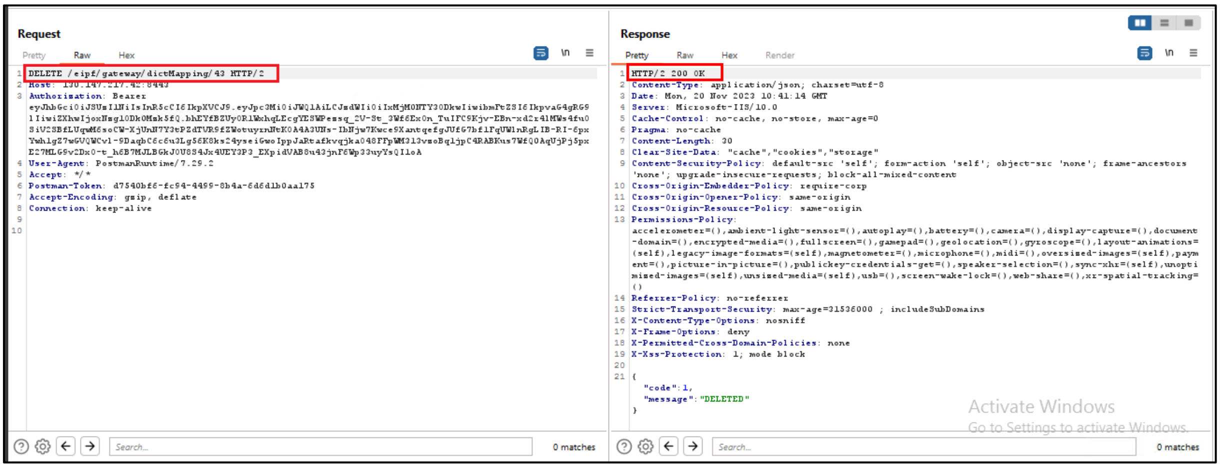
```
POST /eipf/gateway/dictMapping HTTP/2
Host: 130.147.217.42:8443
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJWQ1AiLCJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9
lIiwiZXhwIjoxNzg1ODk0Mzk5fQ.bhEYfBZUy0R1WxhqLEcgYESWPezsq_2V-St_3Wf6Ex0n_TuIFC9Kjv-EBn-xd2r41MWs4fu0
SiV2SBfLUqwM6soCW-XjUnN7Y3tPZdTVR9fZWotuyrnNtK0A4A3UNs-IbNjw7Kwce9XantqefgJUfG7bf1FqUWlnRgLIB-RI-6px
YwhlgZ7wGVQWCvl-9DaqbC6c6u3Lg56K8ks24yseiGwoIppJaRtafkvqjka048FFpWM313vzoBq1jpC4RABKus7WfQ0AqUjPj5px
E27MLG9v2Dx0-t_h6B7MJLBGkJ0U8S4Jx4UEY3P3_EXpidVAB8u43jnF6Wp33uyYsQIloA
Content-Type: application/json
User-Agent: PostmanRuntime/7.29.2
Origin: google.com
Accept: */*
Postman-Token: ebdf4ca6-e989-4fbc-970f-ce6fd1159966
Accept-Encoding: gzip, deflate
Content-Length: 88

{
  "sysCode":"15",
  "value":"unknow",
  "desc":"□□",
  "fkey":1
}
```

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Date: Mon, 20 Nov 2023 10:56:42 GMT
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: *
Cache-Control: no-cache, no-store, max-age=0
Pragma: no-cache
Content-Length: 57
Clear-Site-Data: "cache","cookies","storage"
Content-Security-Policy: default-src 'self'; form-action 'self'; object-src 'none'; frame-ancestors
'none'; upgrade-insecure-requests; block-all-mixed-content
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Permissions-Policy:
accelerometer=(),ambient-light-sensor=(),autoplay=(),battery=(),camera=(),display-capture=(),document
-domain=(),encrypted-media=(),fullscreen=(),gamepad=(),geolocation=(),gyroscope=(),layout-animations=
(self),legacy-image-formats=(self),magnetometer=(),microphone=(),midi=(),oversized-images=(self),paym
ent=(),picture-in-picture=(),publickey-credentials-get=(),speaker-selection=(),sync-xhr=(self),unopti
mized-images=(self),unsized-media=(self),usb=(),screen-wake-lock=(),web-share=(),xr-spatial-tracking=
()
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Content-Type-Options: nosniff
X-Frame-Options: deny
X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 1; mode block

{
  "code":0,
```

7.4 WebServices: Delete method is enabled

Vulnerability Title	Delete method is enabled
Vulnerability Category	A5 Security Misconfiguration
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score:3.7 CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N
Description	**Vulnerability Description:** During the assessment, it is observed that the application server supports DELETE method. While the DELETE method requests that the origin server removes the association between the target resource and its current functionality. **Exploitability rational:** It is relatively difficult to exploit the insecure http methods. **Impact rational:** Improper use of these methods may lead to a loss of integrity.
Affected Systems/IP Address/URL	https://130.147.217.42:8443/eipf/gateway/dictMapping/46
Recommendation	It is recommended to disable unnecesary HTTP Methods.
Status	**Open**

Supportive Evidence:



```
DELETE /eipf/gateway/dictMapping/43 HTTP/2
Host: 130.147.217.42:8443
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJWQ1AiLCJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9
lIiwiZXhwIjoxNzg1ODk0Mzk5fQ.bhEYfBZUy0R1WxhqLEcgYESWPessq_2V-St_3Wf6Ex0n_TuIFC9Kjv-EBn-xd2r41MWs4fu0
SiV2SBfLUqwM6soCW-XjUnN7Y3tPZdTVR9fZWotuyrnNtK0A4A3UNs-IbNjw7Kwce9XantqefgJUfG7bf1FqUWlnRgLIB-RI-6px
Ywh1gZ7wGVQWCvl-9DaqbC6c6u3Lg56K8ks24yseiGwoIppJaRtafkvqjka048FFpWM313vzoBq1jpC4RABKus7WfQ0AqUjPj5px
E27MLG9v2Dx0-t_h6B7MJLBGkJ0U8S4Jx4UEY3P3_EXpidVAB8u43jnF6Wp33uyYsQIloA
User-Agent: PostmanRuntime/7.29.2
Accept: */*
Postman-Token: d7540bf6-fc94-4499-8b4a-6d6d1b0aa175
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Date: Mon, 20 Nov 2023 10:41:14 GMT
Server: Microsoft-IIS/10.0
Cache-Control: no-cache, no-store, max-age=0
Pragma: no-cache
Content-Length: 30
Clear-Site-Data: "cache","cookies","storage"
Content-Security-Policy: default-src 'self'; form-action 'self'; object-src 'none'; frame-ancestors
'none'; upgrade-insecure-requests; block-all-mixed-content
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Permissions-Policy:
accelerometer=(),ambient-light-sensor=(),autoplay=(),battery=(),camera=(),display-capture=(),document
-domain=(),encrypted-media=(),fullscreen=(),gamepad=(),geolocation=(),gyroscope=(),layout-animations=
(self),legacy-image-formats=(self),magnetometer=(),microphone=(),midi=(),oversized-images=(self),paym
ent=(),picture-in-picture=(),publickey-credentials-get=(),speaker-selection=(),sync-xhr=(self),unopti
mized-images=(self),unsized-media=(self),usb=(),screen-wake-lock=(),web-share=(),xr-spatial-tracking=
()
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Content-Type-Options: nosniff
X-Frame-Options: deny
X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 1; mode block

{
  "code":1,
  "message":"DELETED"
}
```

7.5 WebServices: Lack of Input Validation

Vulnerability Title	Lack of Input Validation
Vulnerability Category	A3 Injection
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N
Description	**Vulnerability Description:** During the assessment, it is observed that it allows the usage of special characters. Due to this, the application may be vulnerable to attacks like XSS, SQL injection etc. Input validation is a frequently-used technique for checking potentially dangerous inputs in order to ensure that the inputs are safe for processing within the code, or when communicating with other components. Improper Input Validation in a application can allow an attacker to supply malicious user input that is then executed by the vulnerable web application. Reference: https://cwe.mitre.org/data/definitions/20.html **Exploitability rational:** Failure to properly validate and handle untrusted input represents the single largest category of software security weaknesses. At a minimum, data that is not validated may impact the application's control flow or data flow, leading to unexpected application states for end users, unintended changes to back-end data, as well as unexpected outcomes from executed application logic. An attacker may submit payloads that seek to exploit any number of vulnerabilities that typically result from a lack of input validation. These include (but are not limited to) SQL injection, cross-site scripting, LDAP injection, log injection, and command injection. The consequence of successfully exploiting these vulnerabilities varies, but most provide an attacker with the ability to bypass authentication and/or authorization mechanisms to access, modify or delete application and user data, or execute functionality only available to legitimate user.

	Impact Rational: An attacker can provide unexpected values and cause a program crash or excessive consumption of resources, such as memory and CPU. An attacker can read confidential data if they can control resource references. An attacker can use malicious input to modify data or possibly alter control flow in unexpected ways, including arbitrary command execution.
Affected Systems/IP Address/URL	https://130.147.217.42:8443/eipf/gateway/dictMapping
Recommendation	We recommend the following: • Data that does not match an expected pattern and data that can potentially be used to execute injection attacks must be discarded or sanitized before use. • Perform the validation in such a way that end-users cannot tamper with or bypass the control. Perform the validation on the server-side rather than client-side. Whitelist validation should be favored first over other validation techniques since any character or string not explicitly specified as part of the "known-safe" set of characters or values is rejected or removed by default. Reference: https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
Status	**Open**

Steps to Reproduce

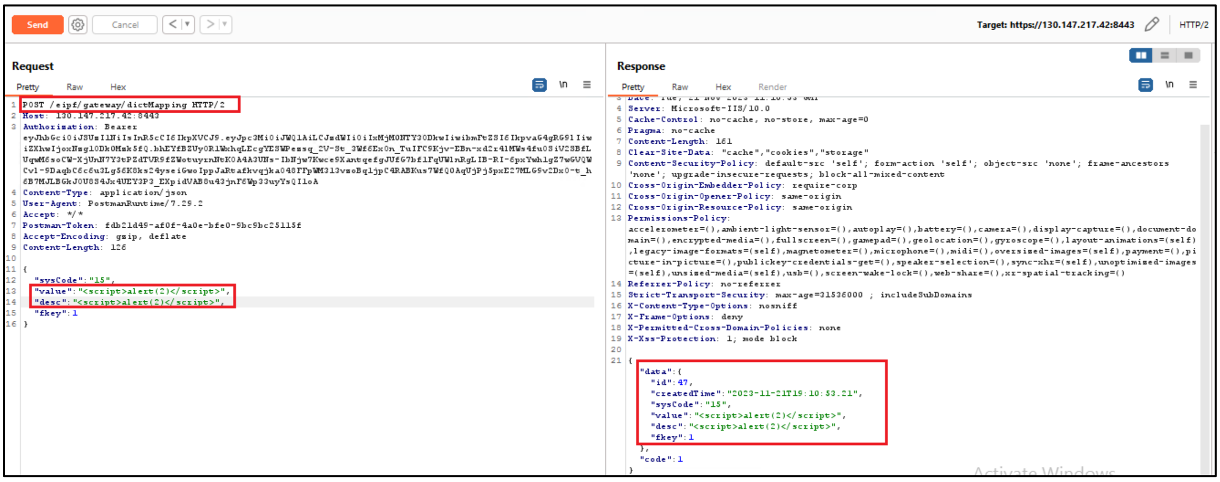
Step 1: Configure postman to work with a proxy tool such as Burp suite.

Step 2: Intercept the request and send to Repeater.

Step 3: Modify some parameters as shown in the screenshot below:

Step 4: Observe the response from the server as shown in the screenshot below:

Supportive Evidence:



```
POST /eipf/gateway/dictMapping HTTP/2
Host: 130.147.217.42:8443
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJWQ1AiLCJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG91IiwiZXhwIjoxNzg1ODk0Mzk5fQ.bhEYfBZUy0R1WxhqLEcgYESWPessq_2V-St_3Wf6Ex0n_TuIFC9Kjv-EBn-xd2r41MWs4fu0SiV2SBfLUqwM6soCW-XjUnN7Y3tPZdTVR9fZWotuyrnNtK0A4A3UNs-IbNjw7Kwce9XantqefgJUfG7bf1FqUWlnRgLIB-RI-6pxYwh1gZ7wGVQWCvl-9DaqbC6c6u3Lg56K8ks24yseiGwoIppJaRtafkvqjka048FFpWM313vsoBq1jpC4RABKus7WfQ0AqUjPj5pxE27MLG9v2Dx0-t_h6B7MJLBGkJ0U8S4Jx4UEY3P3_EXpidVAB8u43jnF6Wp33uyYsQIloA
Content-Type: application/json
User-Agent: PostmanRuntime/7.29.2
Accept: */*
Postman-Token: fdb21d49-af0f-4a0e-bfe0-9bc9bc25115f
Accept-Encoding: gzip, deflate
Content-Length: 126

{
  "sysCode":"15",
  "value":"<script>alert(2)</script>",
  "desc":"<script>alert(2)</script>",
  "fkey":1
}
```

```
Date: Tue, 21 Nov 2023 11:10:53 GMT
Server: Microsoft-IIS/10.0
Cache-Control: no-cache, no-store, max-age=0
Pragma: no-cache
Content-Length: 161
Clear-Site-Data: "cache","cookies","storage"
Content-Security-Policy: default-src 'self'; form-action 'self'; object-src 'none'; frame-ancestors
'none'; upgrade-insecure-requests; block-all-mixed-content
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Permissions-Policy:
accelerometer=(),ambient-light-sensor=(),autoplay=(),battery=(),camera=(),display-capture=(),document-do
main=(),encrypted-media=(),fullscreen=(),gamepad=(),geolocation=(),gyroscope=(),layout-animations=(self)
,legacy-image-formats=(self),magnetometer=(),microphone=(),midi=(),oversized-images=(self),payment=(),pi
cture-in-picture=(),publickey-credentials-get=(),speaker-selection=(),sync-xhr=(self),unoptimized-images
=(self),unsized-media=(self),usb=(),screen-wake-lock=(),web-share=(),xr-spatial-tracking=()
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Content-Type-Options: nosniff
X-Frame-Options: deny
X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 1; mode block

{
  "data":{
    "id":47,
    "createdTime":"2023-11-21T19:10:53.21",
    "sysCode":"15",
    "value":"<script>alert(2)</script>",
    "desc":"<script>alert(2)</script>",
    "fkey":1
  },
  "code":1
}
```

7.6 WebServices: Weak SSL/TLS Configuration

Vulnerability Title	Weak SSL/TLS Configuration
Vulnerability Category	A2 Cryptographic Failures
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.7 CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N
Description	**Vulnerability Description:** During the assessment, it is observed that the application supports to use TLSv1.2 protocols but it allow weak SSL/TLS cipher suites. The following deficiencies were found in the encrypted communication Configuration: - Sweet32 – It uses Collision or “birthday” attack against 64-bit DES/3DES ciphers in CBC mode to decrypt sensitive information like session cookie, by sending large amount of data over a single SSL/TLS session. The server-side SSL/TLS endpoint is configured to allow weak SSL/TLS cipher suites. These cipher suites have proven cryptographic flaws that can allow an attacker to decrypt or modify traffic. References: • https://owasp.org/Top10/A02_2021-Cryptographic_Failures/ • Weak-SSL-TLS-Ciphers-Insufficient-Transport-Layer-Protection **Exploitability rational:** Some misconfigurations in the server can be used to force the use of a weak cipher - or at worst no encryption - permitting to an attacker to gain access to the supposed secure communication channel. Other misconfiguration can be used for a Denial-of-Service attack. **Impact Rational:**

	Sweet32 – An attacker who can send arbitrary HTTP Requests on behalf of the user by controlling the client and can sniff the HTTPS response, is then able to decrypt one block of the encrypted message within 232 attacker-controlled requests.
Affected Systems/IP Address/URL	130.147.217.42
Recommendation	Weak or lowgrade CBC ciphers or encryption must be disabled. Reference: https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html
Status	**Open**

Steps to Reproduce

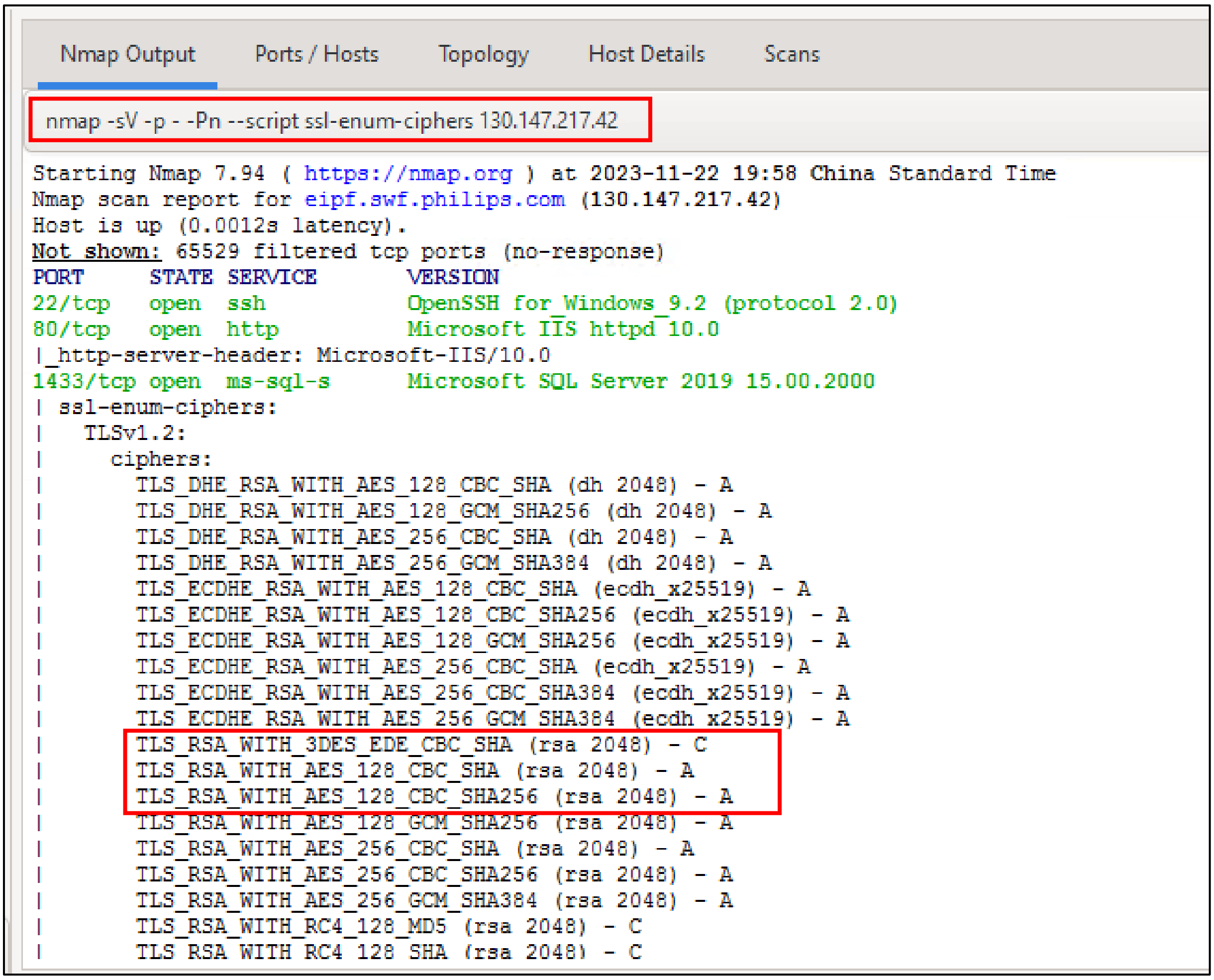
Use tools such as sslscan or nmap to enumerate the ciphers used by the application endpoints.

Step 1: Run the nmap scan:

```
nmap -p 443 -v -Pn --script ssl-enum-ciphers <hostname>
```

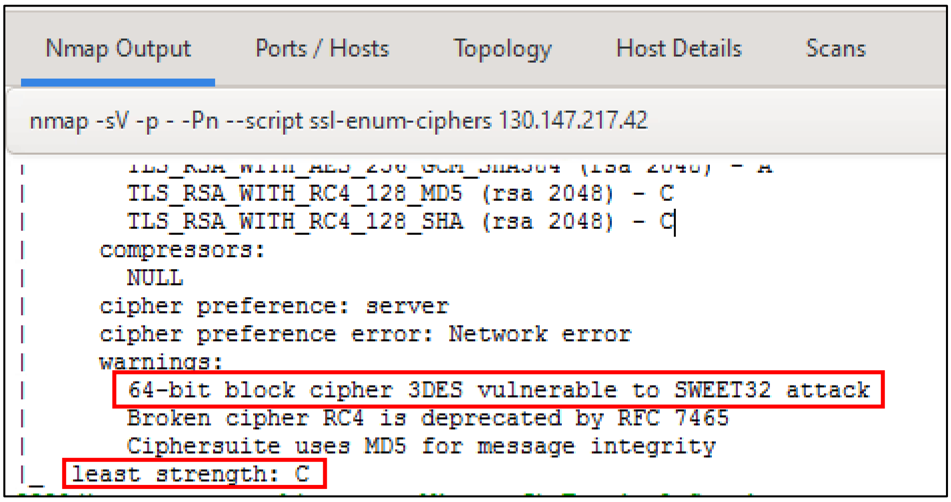
Step 2: Observe the result that application uses weak ciphers.

Supportive Evidence:



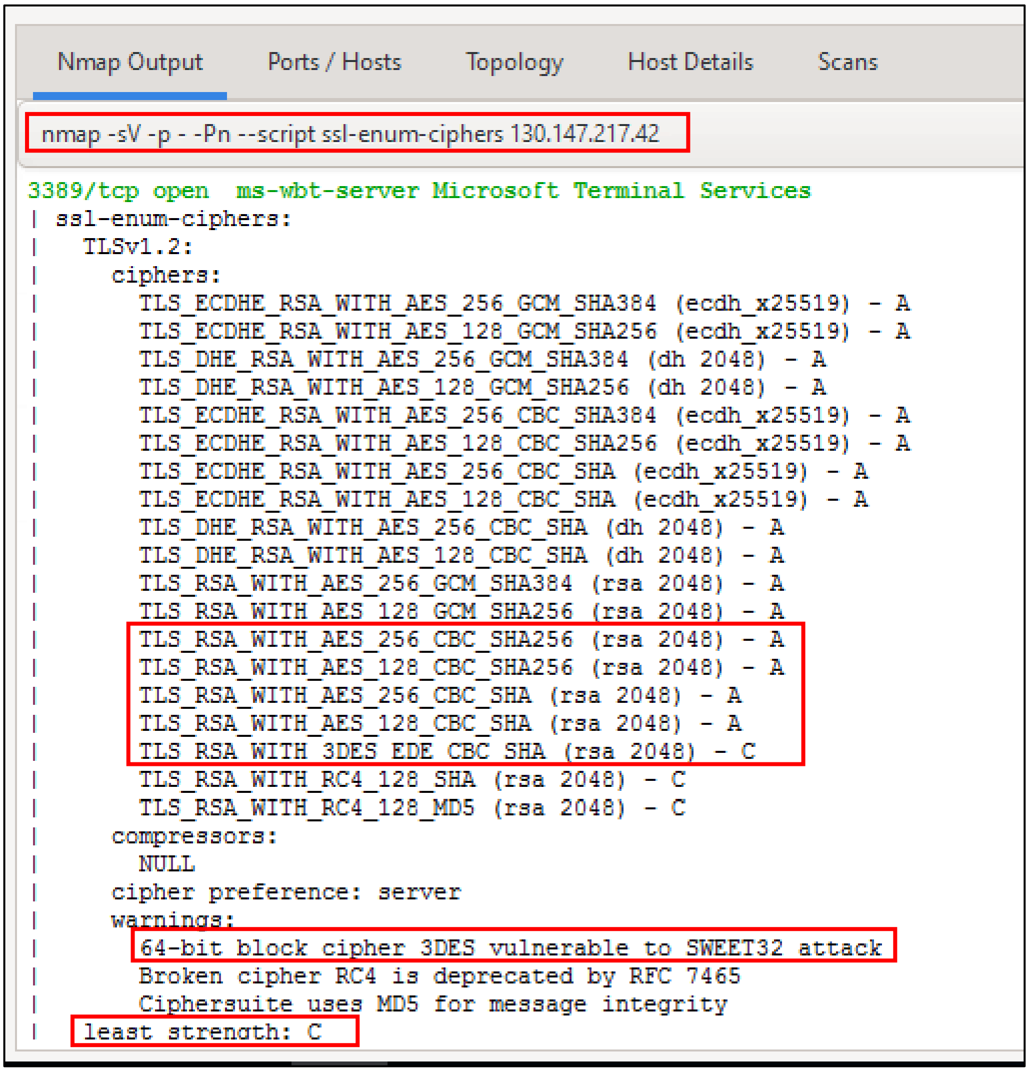
```
nmap -sV -p - -Pn --script ssl-enum-ciphers 130.147.217.42
```

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-22 19:58 China Standard Time
Nmap scan report for eipf.swf.philips.com (130.147.217.42)
Host is up (0.0012s latency).
Not shown: 65529 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH for_Windows_9.2 (protocol 2.0)
80/tcp   open  http        Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
1433/tcp open  ms-sql-s    Microsoft SQL Server 2019 15.00.2000
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
```



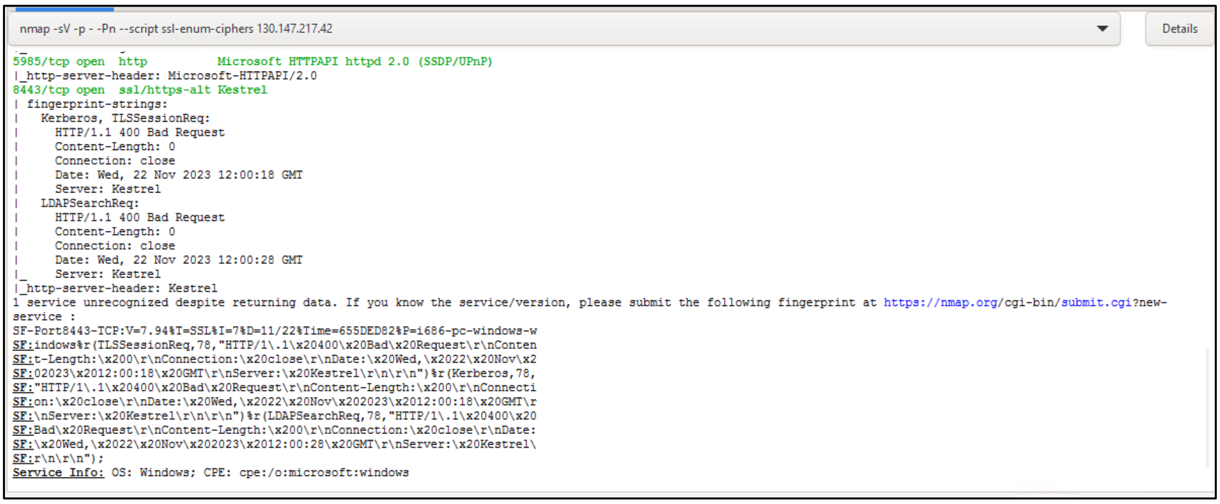
```
nmap -sV -p - -Pn --script ssl-enum-ciphers 130.147.217.42
```

```
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     cipher preference error: Network error
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|_  least strength: C
```



```
nmap -sV -p - -Pn --script ssl-enum-ciphers 130.147.217.42
```

```
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|   least strength: C
```



```
nmap -sV -p - -Pn --script ssl-enum-ciphers 130.147.217.42
```

```
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
8443/tcp open  ssl/https-alt Kestrel
| fingerprint-strings:
|   Kerberos, TLSSessionReq:
|     HTTP/1.1 400 Bad Request
|     Content-Length: 0
|     Connection: close
|     Date: Wed, 22 Nov 2023 12:00:18 GMT
|     Server: Kestrel
|   LDAPSearchReq:
|     HTTP/1.1 400 Bad Request
|     Content-Length: 0
|     Connection: close
|     Date: Wed, 22 Nov 2023 12:00:28 GMT
|_    Server: Kestrel
|_http-server-header: Kestrel
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-
service :
SF-Port8443-TCP:V=7.94%T=SSL%I=7%D=11/22%Time=655DED82%P=i686-pc-windows-w
SF:indows%r(TLSSessionReq,78,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConten
SF:t-Length:\x200\r\nConnection:\x20close\r\nDate:\x20Wed,\x2022\x20Nov\x2
SF:02023\x2012:00:18\x20GMT\r\nServer:\x20Kestrel\r\n\r\n")%r(Kerberos,78,
SF:"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Length:\x200\r\nConnecti
SF:on:\x20close\r\nDate:\x20Wed,\x2022\x20Nov\x202023\x2012:00:18\x20GMT\r
SF:\nServer:\x20Kestrel\r\n\r\n")%r(LDAPSearchReq,78,"HTTP/1\.1\x20400\x20
SF:Bad\x20Request\r\nContent-Length:\x200\r\nConnection:\x20close\r\nDate:
SF:\x20Wed,\x2022\x20Nov\x202023\x2012:00:28\x20GMT\r\nServer:\x20Kestrel\
SF:r\n\r\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

7.7 WebServices: Verbose Server Banner

Vulnerability Title	Verbose Server Banner
Vulnerability Category	A5 Security Misconfiguration
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.1 CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N
Description	**Vulnerability Description:** During the security assessment, it was found that the application discloses the application server details including the version in the HTTP response. Targeted attacks can be launched against the server based on the exploits it is having. References: • https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server • https://www.tenable.com/plugins/was/98618 **Exploitability rational:** Web server fingerprinting is a critical task for the penetration tester. Knowing the version and type of a running web server allows testers to determine known vulnerabilities and the appropriate exploits to use during testing and those are available on internet. **Impact rational:** Targeted attacks can be launched against the server based on the exploits it is having.
Affected Systems/IP Address/URL	https://130.147.217.42:8443/eipf/gateway/dictMapping
Recommendation	It is recommended to use custom banner for server by hiding all sensitive information from banner.

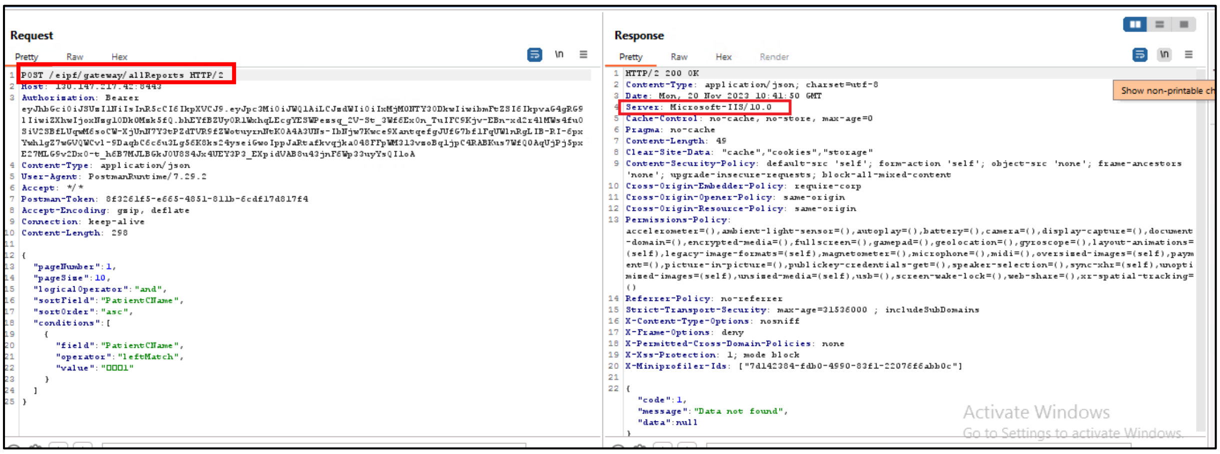
	https://techcommunity.microsoft.com/t5/iis-support-blog/remove-unwanted-http-response-headers/ba-p/369710
Status	**Open**

Steps to Reproduce

Step 1: Use a proxy tool like Burp Suite to capture any request.

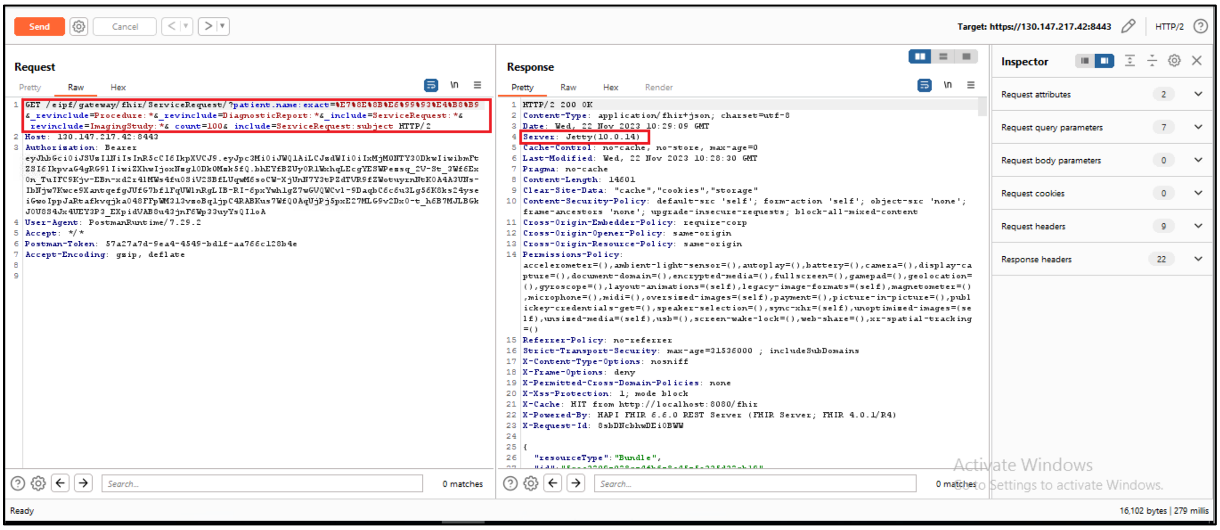
Step 2: Observe that the http response is disclosing server name and its version as shown in the screenshot below:

Supportive Evidence:



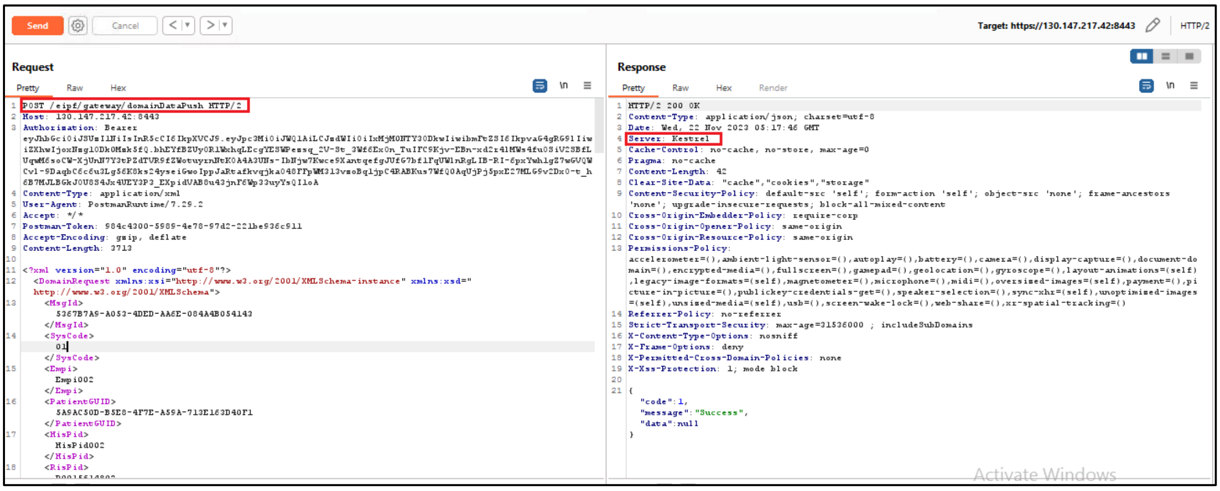
```
POST /eipf/gateway/allReports HTTP/2
Host: 130.147.217.42:8443
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJWQ1AiLCJsdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9
1IiwiZXhwIjoxNsg1ODk0Msk5fQ.bhEYfBZUy0R1WxhqLEcgYESWPessq_2V-St_3Wf6Ex0n_TuIFC9Kjv-EBn-xd2r41MWs4fu0
SiV2SBfLUqwM6soCW-XjUnN7Y3tPZdTVR9fZWotuyrnNtK0A4A3UNs-IbNjw7Kwce9XantqefgJUfG7bf1FqUWlnRgLIB-RI-6px
Ywhlgz7wGVQWCvl-9DaqbC6c6u3Lg56K8ks24yseiGwoIppJaRtafkvqjka048FFpWM313vsoBqljpC4RABKus7WfQ0AqUjPj5px
E27MLG9v2Dx0-t_h6B7MJLBGkJ0U8S4Jx4UEY3P3_EXpidVAB8u43jnF6Wp33uyYsQIloA
Content-Type: application/json
User-Agent: PostmanRuntime/7.29.2
Accept: */*
Postman-Token: 8f3261f5-e665-4851-811b-6cdf17d817f4
Accept-Encoding: gzip, deflate
Connection: keep-alive
Content-Length: 298

{
  "pageNumber":1,
  "pageSize":10,
  "logicalOperator":"and",
  "sortField":"PatientCName",
  "sortOrder":"asc",
  "conditions":[
    {
      "field":"PatientCName",
      "operator":"leftMatch",
      "value":"OOO1"
    }
  ]
}
```

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Date: Mon, 20 Nov 2023 10:41:50 GMT
Server: Microsoft-IIS/10.0
Cache-Control: no-cache, no-store, max-age=0
Pragma: no-cache
Content-Length: 49
Clear-Site-Data: "cache","cookies","storage"
Content-Security-Policy: default-src 'self'; form-action 'self'; object-src 'none'; frame-ancestors
'none'; upgrade-insecure-requests; block-all-mixed-content
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Permissions-Policy:
accelerometer=(),ambient-light-sensor=(),autoplay=(),battery=(),camera=(),display-capture=(),document
-domain=(),encrypted-media=(),fullscreen=(),gamepad=(),geolocation=(),gyroscope=(),layout-animations=
(self),legacy-image-formats=(self),magnetometer=(),microphone=(),midi=(),oversized-images=(self),paym
ent=(),picture-in-picture=(),publickey-credentials-get=(),speaker-selection=(),sync-xhr=(self),unopti
mized-images=(self),unsized-media=(self),usb=(),screen-wake-lock=(),web-share=(),xr-spatial-tracking=
()
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Content-Type-Options: nosniff
X-Frame-Options: deny
X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 1; mode block
X-Miniprofiler-Ids: ["7d142384-fdb0-4990-83f1-22076f6abb0c"]

{
  "code":1,
  "message":"Data not found",
  "data":null
}
```



```
GET /eipf/gateway/fhir/ServiceRequest/?patient.name:exact=%E7%8E%8B%E6%99%93%E4%B8%B9
&_revinclude=Procedure:*&_revinclude=DiagnosticReport:*&_include=ServiceRequest:*&
_revinclude=ImagingStudy:*&_count=100&_include=ServiceRequest:subject HTTP/2
Host: 130.147.217.42:8443
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJWQ1AiLCJsdWIiOiIxMjM0NTY3ODkwIiwibmFt
ZSI6IkpvaG4gRG91IiwiZXhwIjoxNsg1ODk0Msk5fQ.bhEYfBZUy0R1WxhqLEcgYESWPessq_2V-St_3Wf6Ex
0n_TuIFC9Kjv-EBn-xd2r41MWs4fu0SiV2SBfLUqwM6soCW-XjUnN7Y3tPZdTVR9fZWotuyrnNtK0A4A3UNs-
IbNjw7Kwce9XantqefgJUfG7bf1FqUWlnRgLIB-RI-6pxYwhlgZ7wGVQWCvl-9DaqbC6c6u3Lg56K8ks24yse
iGwoIppJaRtafkvqjka048FFpWM313vsoBqljpC4RABKus7WfQ0AqUjPj5pxE27MLG9v2Dx0-t_h6B7MJLBGk
J0U8S4Jx4UEY3P3_EXpidVAB8u43jnF6Wp33uyYsQIloA
User-Agent: PostmanRuntime/7.29.2
Accept: */*
Postman-Token: 57a27a7d-9ea4-4549-bd1f-aa766c128b4e
Accept-Encoding: gzip, deflate
```

```
HTTP/2 200 OK
Content-Type: application/fhir+json; charset=utf-8
Date: Wed, 22 Nov 2023 10:29:09 GMT
Server: Jetty(10.0.14)
Cache-Control: no-cache, no-store, max-age=0
Last-Modified: Wed, 22 Nov 2023 10:28:30 GMT
Pragma: no-cache
Content-Length: 14601
Clear-Site-Data: "cache","cookies","storage"
Content-Security-Policy: default-src 'self'; form-action 'self'; object-src 'none';
frame-ancestors 'none'; upgrade-insecure-requests; block-all-mixed-content
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Permissions-Policy:
accelerometer=(),ambient-light-sensor=(),autoplay=(),battery=(),camera=(),display-ca
pture=(),document-domain=(),encrypted-media=(),fullscreen=(),gamepad=(),geolocation=
(),gyroscope=(),layout-animations=(self),legacy-image-formats=(self),magnetometer=()
,microphone=(),midi=(),oversized-images=(self),payment=(),picture-in-picture=(),publ
ickey-credentials-get=(),speaker-selection=(),sync-xhr=(self),unoptimized-images=(se
lf),unsized-media=(self),usb=(),screen-wake-lock=(),web-share=(),xr-spatial-tracking
=()
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Content-Type-Options: nosniff
X-Frame-Options: deny
X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 1; mode block
X-Cache: HIT from http://localhost:8080/fhir
X-Powered-By: HAPI FHIR 6.6.0 REST Server (FHIR Server; FHIR 4.0.1/R4)
X-Request-Id: 8sbDNcbhwDEi0BWW

{
  "resourceType":"Bundle",
```



```
POST /eipf/gateway/domainDataPush HTTP/2
Host: 130.147.217.42:8443
Authorization: Bearer
eyJhbGci0iJSUsI1NiIsInR5cCI6IkpXVCJ9.eyJpc3Mi0iJWQ1AiLCJsdWIi0iIxMjM0NTY30DkwIiwibmFtZSI6IkpvaG4gRG9lIiw
iZXhwIjoxNsg10Dk0Msk5fQ.bhEYfBZUy0R1WxhqLEcgYESWPessq_2V-St_3Wf6Ex0n_TuIFC9Kjv-EBn-xd2r41MWs4fu0SiV2SBfL
UqwM6soCW-XjUnN7Y3tPZdTVR9fZWotuyrnNtK0A4A3UNs-IbNjw7Kwce9XantqefgJUfG7bf1FqUWlnRgLIB-RI-6pxYwh1gZ7wGVQW
Cvl-9DaqbC6c6u3Lg56K8ks24yseiGwoIppJaRtafkvqjka048FFpWM313vsoBq1jpC4RABKus7WfQ0AqUjPj5pxE27MLG9v2Dx0-t_h
6B7MJLBGkJ0U8S4Jx4UEY3P3_EXpidVAB8u43jnF6Wp33uyYsQIloA
Content-Type: application/xml
User-Agent: PostmanRuntime/7.29.2
Accept: */*
Postman-Token: 984c4300-5989-4e78-97d2-221be936c911
Accept-Encoding: gsip, deflate
Content-Length: 3713

<?xml version="1.0" encoding="utf-8"?>
  <DomainRequest xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="
  http://www.w3.org/2001/XMLSchema">
    <MsgId>
      5367B7A9-A053-4DED-AA6E-084A4B054143
    </MsgId>
    <SysCode>
      01
    </SysCode>
    <Empi>
      Empi002
    </Empi>
    <PatientGUID>
      5A9AC50D-B5E8-4F7E-A59A-713E163D40F1
    </PatientGUID>
    <HisPid>
      HisPid002
    </HisPid>
    <RisPid>
```

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Date: Wed, 22 Nov 2023 05:17:46 GMT
Server: Kestrel
Cache-Control: no-cache, no-store, max-age=0
Pragma: no-cache
Content-Length: 42
Clear-Site-Data: "cache","cookies","storage"
Content-Security-Policy: default-src 'self'; form-action 'self'; object-src 'none'; frame-ancestors
'none'; upgrade-insecure-requests; block-all-mixed-content
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Permissions-Policy:
accelerometer=(),ambient-light-sensor=(),autoplay=(),battery=(),camera=(),display-capture=(),document-do
main=(),encrypted-media=(),fullscreen=(),gamepad=(),geolocation=(),gyroscope=(),layout-animations=(self)
,legacy-image-formats=(self),magnetometer=(),microphone=(),midi=(),oversized-images=(self),payment=(),pi
cture-in-picture=(),publickey-credentials-get=(),speaker-selection=(),sync-xhr=(self),unoptimized-images
=(self),unsized-media=(self),usb=(),screen-wake-lock=(),web-share=(),xr-spatial-tracking=()
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Content-Type-Options: nosniff
X-Frame-Options: deny
X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 1; mode block

{
  "code":1,
  "message":"Success",
  "data":null
}
```

7.8 WebServices: Improper Error Handling

Vulnerability Title	Improper Error Handling
Vulnerability Category	A5 Security Misconfiguration
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.4 CVSS:3.1/AV:A/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N
Description	**Vulnerability Description:** Improper handling of errors can introduce a variety of security problems for a web site. The most common problem is when detailed internal error messages such as stack traces, database dumps, and error codes are displayed to the user (attacker). These messages reveal implementation details which are supposed to be hidden. Reference: https://owasp.org/www-community/Improper_Error_Handling **Exploitability rational:** An attacker should have access to the application. **Impact rational:** By leveraging the verbose error an attacker can gain more information about the target which help in fine tuning his/her future attack.
Affected Systems/IP Address/URL	https://130.147.217.42:8443/eipf/gateway/dictMapping
Recommendation	The application should return customized generic error messages to the user's browser. If details about the error are needed for debugging or support reasons a unique identifier may be created and displayed to the user along with the generic error message for reference. This same unique identifier can be included with the error that is logged to the server so that it can be easily correlated with the issue.

	References: • https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html • Improper-Error-Handling-Fix-In-JAVA • Improper-Error-Handling-Fix-In-ASP.NET-Core • Improper-Error-Handling-Fix-In-SpringBoot
Status	**Open**

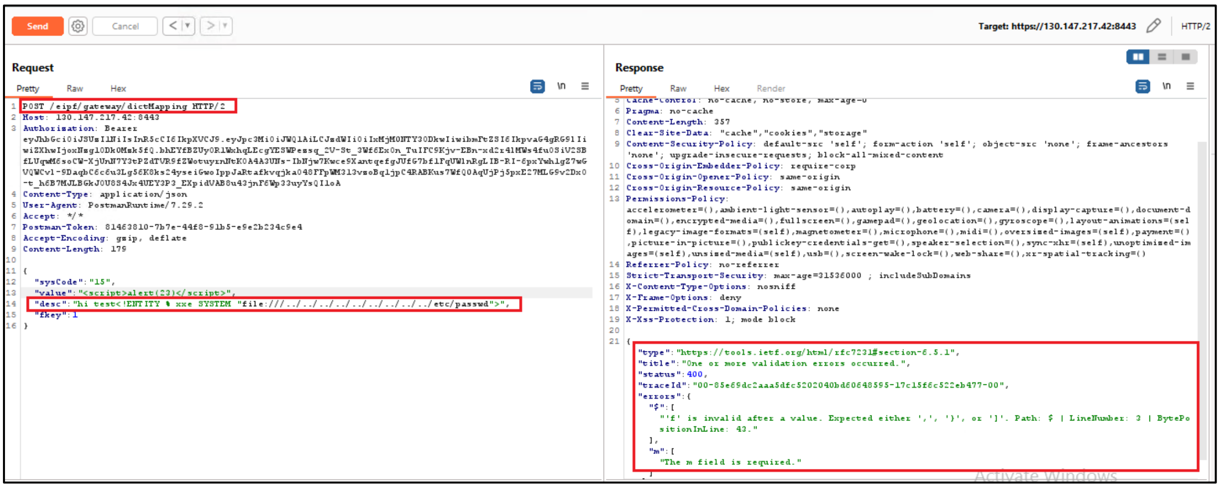
Steps to Reproduce

Step 1: Configure the browser to use proxy tool such as Burp Suite.

Step 2: Capture a request containing some input fields and send it to the Repeater tool.

Step 3: Manipulate the request with certain malicious characters in the input fields and observe that there is error disclosure in the response as shown in the screenshot below:

Supportive Evidence:



```
POST /eipf/gateway/dictMapping HTTP/2
Host: 130.147.217.42:8443
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJWQ1AiLCJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIi
wiZXhwIjoxNzg1ODk0Mzk5fQ.bhEYfBZUy0R1WxhqLEcgYESWPezsq_2V-St_3Wf6Ex0n_TuIFC9Kjv-EBn-xd2r41MWs4fu0SiV2SB
fLUqwM6soCW-XjUnN7Y3tPZdTVR9fZWotuyrnNtK0A4A3UNs-IbNjw7Kwce9XantqefgJUfG7bf1FqUWlnRgLIB-RI-6pxYwh1gZ7wG
VQWCvl-9DaqbC6c6u3Lg56K8ks24yseiGwoIppJaRtafkvqjka048FFpWM313vzoBq1jpC4RABKus7WfQ0AqUjPj5pxE27MLG9v2Dx0
-t_h6B7MJLBGkJ0U834Jx4UEY3P3_EXpidVAB8u43jnF6Wp33uyYsQIloA
Content-Type: application/json
User-Agent: PostmanRuntime/7.29.2
Accept: */*
Postman-Token: 81463810-7b7e-44f8-91b5-e9e2b234c9e4
Accept-Encoding: gzip, deflate
Content-Length: 179

{
  "sysCode":"15",
  "value":"<script>alert(23)</script>",
  "desc":"hi test<!ENTITY % xxe SYSTEM "file:///../../../../../../../../../etc/passwd">",
  "fkey":1
}
```

```
Cache-Control: no-cache, no-store, max-age=0
Pragma: no-cache
Content-Length: 357
Clear-Site-Data: "cache","cookies","storage"
Content-Security-Policy: default-src 'self'; form-action 'self'; object-src 'none'; frame-ancestors
'none'; upgrade-insecure-requests; block-all-mixed-content
Cross-Origin-Embedder-Policy: require-corp
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
Permissions-Policy:
accelerometer=(),ambient-light-sensor=(),autoplay=(),battery=(),camera=(),display-capture=(),document-d
omain=(),encrypted-media=(),fullscreen=(),gamepad=(),geolocation=(),gyroscope=(),layout-animations=(sel
f),legacy-image-formats=(self),magnetometer=(),microphone=(),midi=(),oversized-images=(self),payment=()
,picture-in-picture=(),publickey-credentials-get=(),speaker-selection=(),sync-xhr=(self),unoptimized-im
ages=(self),unsized-media=(self),usb=(),screen-wake-lock=(),web-share=(),xr-spatial-tracking=()
Referrer-Policy: no-referrer
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Content-Type-Options: nosniff
X-Frame-Options: deny
X-Permitted-Cross-Domain-Policies: none
X-Xss-Protection: 1; mode block

{
  "type":"https://tools.ietf.org/html/rfc7231#section-6.5.1",
  "title":"One or more validation errors occurred.",
  "status":400,
  "traceId":"00-85e69dc2aaa5dfc5202040bd60648595-17c15f6c522eb477-00",
  "errors":{
    "$":[
      "'f' is invalid after a value. Expected either ',', '}', or ']'. Path: $ | LineNumber: 3 | BytePo
      sitionInLine: 43."
    ],
    "m":[
      "The m field is required."
    ]
```

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

7.9 Windows Services: Sensitive Data in Memory

Vulnerability Title	Sensitive Data in Memory
Vulnerability Category	Others
Severity	**Medium**
CVSS V3 Calculation	CVSS Base Score: 5.9 CVSS:3.1/AV:P/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:L
Description	**Vulnerability Description:** Thick Client application temporarily stores data into the memory from different environments like users or network for further processing. This type of data includes usernames, passwords, connection strings or any other sensitive data. Thick client application generally has a user authentication form, where user supplies username and password as credentials. These credentials are stored in the memory for future processing by the application. To validate these credentials, application fetches correct username & password from the database. This actual username & password is also stored temporarily in the memory. These credentials stay in the memory until they get overwritten by any other data. **Exploitability Rational:** Any attacker that has physical access to the machine can exploit this vulnerability. **Impact Rational:** Any attacker that has access to this information can impersonate any user that uses the application by obtaining their user credentials.
Affected Systems/IP Address/URL	HSC.EIPF.FhirSyncService.exe
Recommendation	Clear the memory area that contains critical data after a sensitive action. This means application should clear the username and password from the memory after authentication process. This ensures that further a malicious user cannot retrieve any sensitive data from the memory.
Status	**Open**

Steps to Reproduce

Step 1: Launch the FhirSyncService.

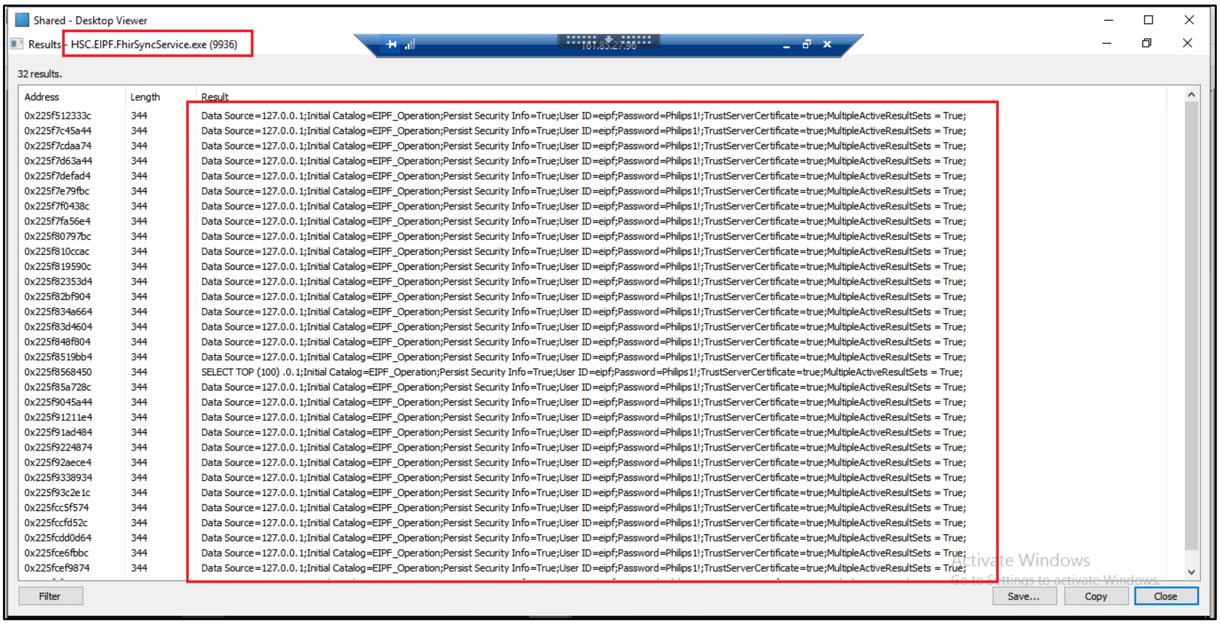
Step 2: Launch the process hacker tool and select the HSC.EIPF.FhirSyncService.exe process in the tool.

Step 3: Right click > Properties > Memory and filter the strings with minimum 3 characters.

Step 4: Search for case insensitive string like Password/UserID.

Step 5: Observe that the password/userid is found in memory as shown in the below screenshot:

Supportive Evidence:



Results - HSC.EIPF.FhirSyncService.exe (9936)

32 results.

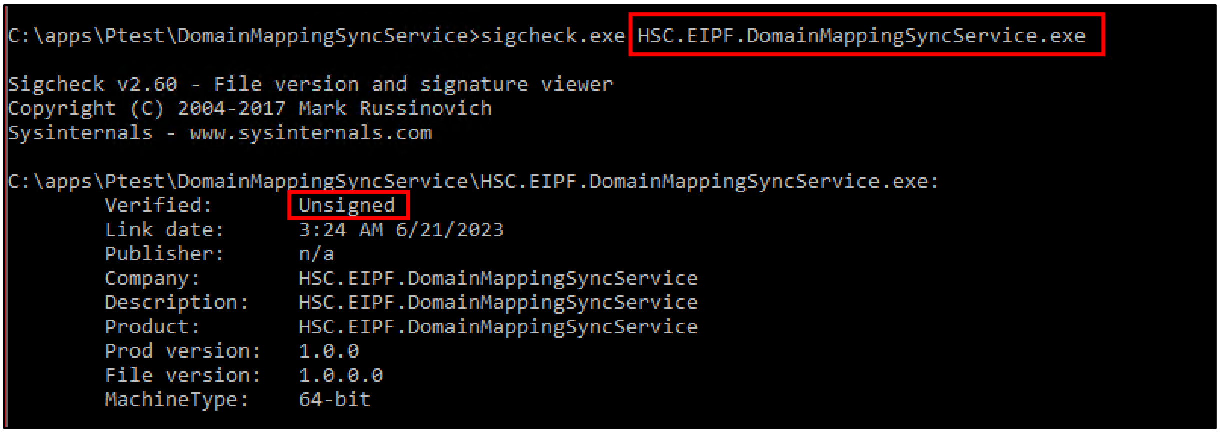
Address	Length	Result
0x225f512333c	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f7c45a44	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f7cdaa74	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f7d63a44	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f7defad4	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f7e79fbc	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f7f0438c	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f7fa56e4	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f80797bc	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f810ccac	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f819590c	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f82353d4	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f82bf904	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f834a664	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f83d4604	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f848f804	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f8519bb4	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f8568450	344	SELECT TOP (100) .0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f85a728c	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f9045a44	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f91211e4	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f91ad484	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f9224874	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f92aece4	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f9338934	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225f93c2e1c	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225fcc5f574	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225fccfd52c	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225fcdd0d64	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225fce6fbbc	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;
0x225fcef9874	344	Data Source=127.0.0.1;Initial Catalog=EIPF_Operation;Persist Security Info=True;User ID=eipf;Password=Philips1!;TrustServerCertificate=true;MultipleActiveResultSets = True;

HSC.EIPF.FhirSyncService.exe

7.10 WindowsServices: Unsigned Binaries

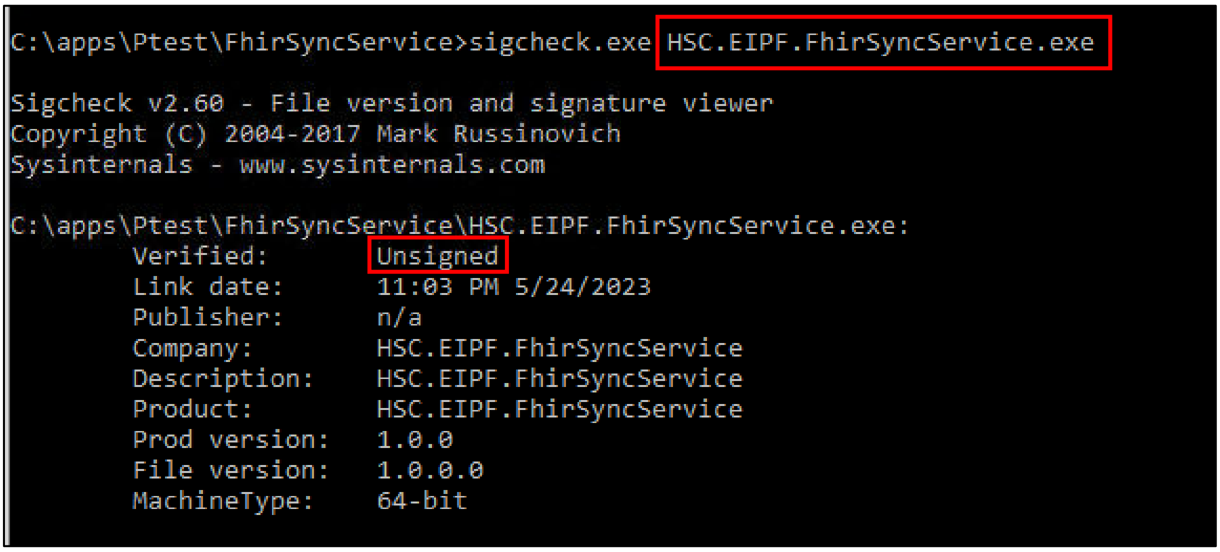
Vulnerability Title	Unsigned Binaries
Vulnerability Category	Others
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 2.9 CVSS:3.0/AV:L/AC:H/PR:H/UI:R/S:C/C:L/I:L/A:N
Description	**Vulnerability Description:** During the security assessment of the product, it is observed many of the binaries do not have a valid signature. Code signing with a developer certificate provides authenticity, reputation and integrity to the code and application. **Exploitability Rational:** An attacker needs local access to the system to exploit this issue. **Impact Rational:** A successful attack could result in execution of attacker injected code. Reference: https://msdn.microsoft.com/enus/library/ms537361(v=vs.85).aspx
Affected Systems/IP Address/URL	C:\apps\Ptest\DomainMappingSyncService\HSC.EIPF.DomainMappingSyncService.exe C:\apps\Ptest\FhirSyncService\HSC.EIPF.FhirSyncService.exe C:\apps\Ptest\HSC.EIPF.NotificationService.V6\HSC.EIPF.NotificationService.exe
Recommendation	It is recommended to sign the code with a developer certificate. Use Microsoft Sign Tool for signing executables. Executable must be signed by valid CA authority.
Status	**Open**

Supportive Evidence:



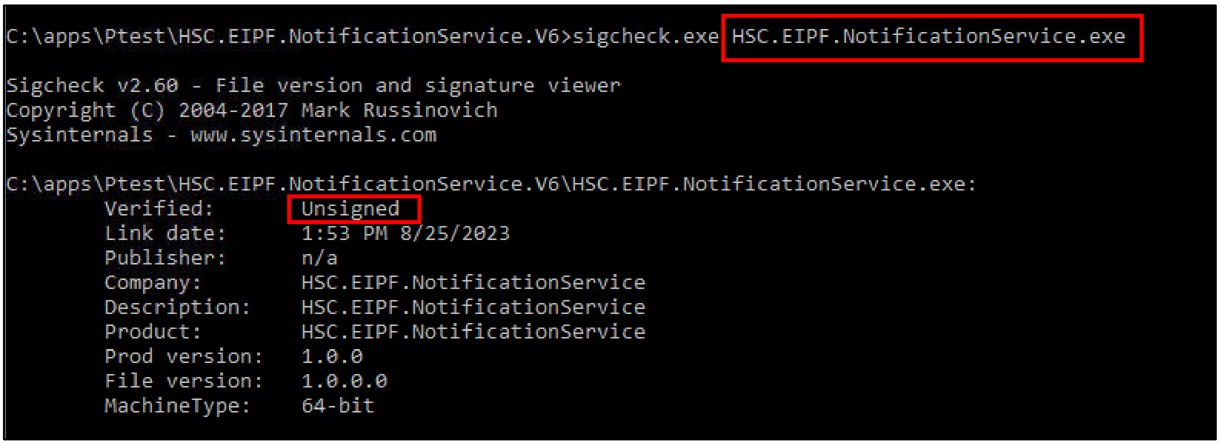
```
C:\apps\Ptest\DomainMappingSyncService>sigcheck.exe HSC.EIPF.DomainMappingSyncService.exe

Sigcheck v2.60 - File version and signature viewer
Copyright (C) 2004-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\apps\Ptest\DomainMappingSyncService\HSC.EIPF.DomainMappingSyncService.exe:
        Verified:       Unsigned
        Link date:      3:24 AM 6/21/2023
        Publisher:      n/a
        Company:        HSC.EIPF.DomainMappingSyncService
        Description:    HSC.EIPF.DomainMappingSyncService
        Product:        HSC.EIPF.DomainMappingSyncService
        Prod version:   1.0.0
        File version:   1.0.0.0
        MachineType:    64-bit
```

It is observed that application EXE’s are unsigned.



```
C:\apps\Ptest\FhirSyncService>sigcheck.exe HSC.EIPF.FhirSyncService.exe

Sigcheck v2.60 - File version and signature viewer
Copyright (C) 2004-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\apps\Ptest\FhirSyncService\HSC.EIPF.FhirSyncService.exe:
        Verified:       Unsigned
        Link date:      11:03 PM 5/24/2023
        Publisher:      n/a
        Company:        HSC.EIPF.FhirSyncService
        Description:    HSC.EIPF.FhirSyncService
        Product:        HSC.EIPF.FhirSyncService
        Prod version:   1.0.0
        File version:   1.0.0.0
        MachineType:    64-bit
```

It is observed that application EXE’s are unsigned.



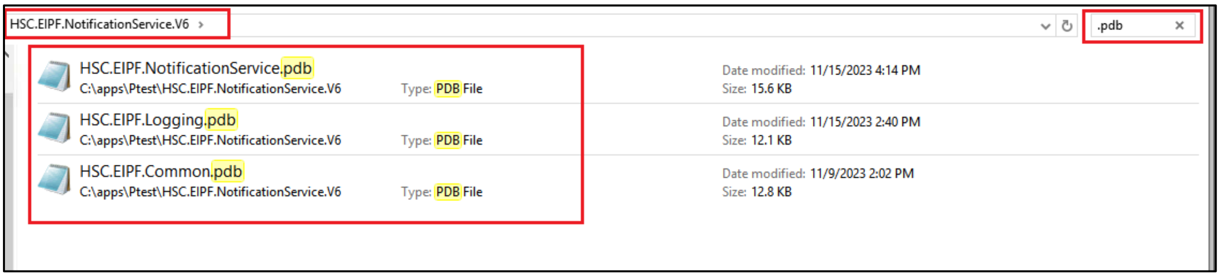
```
C:\apps\Ptest\HSC.EIPF.NotificationService.V6>sigcheck.exe HSC.EIPF.NotificationService.exe

Sigcheck v2.60 - File version and signature viewer
Copyright (C) 2004-2017 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\apps\Ptest\HSC.EIPF.NotificationService.V6\HSC.EIPF.NotificationService.exe:
        Verified:       Unsigned
        Link date:      1:53 PM 8/25/2023
        Publisher:      n/a
        Company:        HSC.EIPF.NotificationService
        Description:    HSC.EIPF.NotificationService
        Product:        HSC.EIPF.NotificationService
        Prod version:   1.0.0
        File version:   1.0.0.0
        MachineType:    64-bit
```

It is observed that application EXE's are unsigned.

7.11 WindowsServices: PDB files included in the Binary

Vulnerability Title	PDB files included in the Binary
Vulnerability Category	Others
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 2.5 CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N
Description	**Vulnerability Description:** During security assessment, it was observed that the binary had pdb files unremoved. The pdb files are the symbol files that are the final product of the compiled source code used for debugging purpose. **Exploitability Rational:** The attacker needs to be a local account user to fetch the information. **Impact Rational:** An attacker who shall access these files could understand the product better and plan for further attacks.
Affected Systems/IP Address/URL	C:\apps\Ptest\HSC.EIPF.NotificationService.V6\HSC.EIPF.NotificationService.exe
Recommendation	It is recommended to remove any unwanted files post development and prior to production release.
Status	**Open**

Supportive Evidence:



HSC.EIPF.NotificationService.V6 >

.pdb ×

HSC.EIPF.NotificationService.pdb
C:\apps\Ptest\HSC.EIPF.NotificationService.V6
Type: PDB File
Date modified: 11/15/2023 4:14 PM
Size: 15.6 KB

HSC.EIPF.Logging.pdb
C:\apps\Ptest\HSC.EIPF.NotificationService.V6
Type: PDB File
Date modified: 11/15/2023 2:40 PM
Size: 12.1 KB

HSC.EIPF.Common.pdb
C:\apps\Ptest\HSC.EIPF.NotificationService.V6
Type: PDB File
Date modified: 11/9/2023 2:02 PM
Size: 12.8 KB

7.12 WindowsServices: DLL Injection

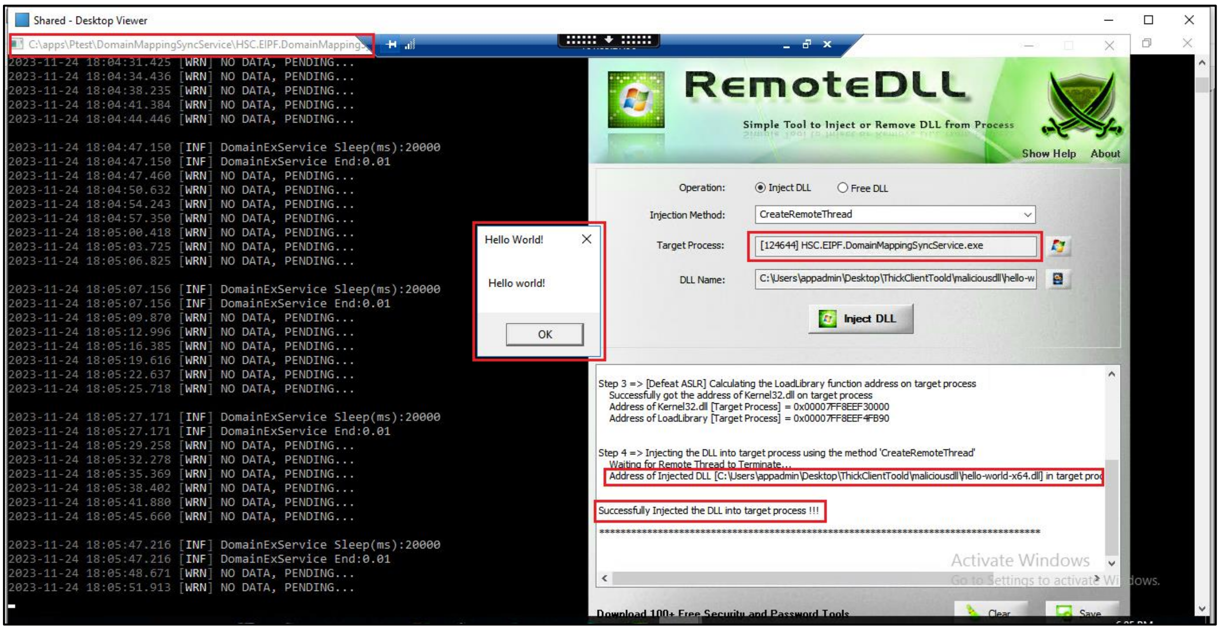
Vulnerability Title	DLL Injection
Vulnerability Category	Others
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 2.9 CVSS:3.1/AV:P/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L
Description	**Vulnerability Description:** DLL injection is a technique, which allows an attacker to run arbitrary code in the context of the address space of another process. If this process is running with low privileges, then an attacker could abuse it to execute malicious code in the form of a DLL file to elevate privileges. Reference: https://owasp.org/www-community/attacks/Binary_planting **Exploitability Rational:** The attacker requires access to find the running process of the application. **Impact Rational:** Once the application executes the malicious DLL it can perform malicious task on the server.
Affected Systems/IP Address/URL	HSC.EIPF.DomainMappingSyncService.exe HSC.EIPF.FhirSyncService.exe HSC.EIPF.NotificationService.exe
Recommendation	• Ensure that the application only loads DLL, which are legitimate from the whitelisted DLL's and deny access to other DLL other than the list. • One need to ensure no untrusted process gets Administrator access or runs as the same user account as your application.
Status	**Open**

Steps to reproduce

Step 1: We have created a DLL, which will execute a pop up for test purpose. Similarly, we can write to perform various malicious activities. In our case the DLL name is “hello-world-x64.dll”.

Step 2: Using RemoteDLL 64bit tool, inject the DLL into the application process. Observe that the application executes the malicious DLL. Similarly, any malicious task can be executed on the system.

Supportive Evidence:



Shared - Desktop Viewer
C:\apps\Ptest\DomainMappingSyncService\HSC.EIPF.DomainMapping
RemoteDLL
Simple Tool to Inject or Remove DLL from Process
Show Help
About
Inject DLL
Download 100+ Free Security and Password Tools
Clear
Save
Activate Windows
Go to Settings to activate Windows.

```
2023-11-24 18:04:31.425 [WRN] NO DATA, PENDING...
2023-11-24 18:04:34.436 [WRN] NO DATA, PENDING...
2023-11-24 18:04:38.235 [WRN] NO DATA, PENDING...
2023-11-24 18:04:41.384 [WRN] NO DATA, PENDING...
2023-11-24 18:04:44.446 [WRN] NO DATA, PENDING...

2023-11-24 18:04:47.150 [INF] DomainExService Sleep(ms):20000
2023-11-24 18:04:47.150 [INF] DomainExService End:0.01
2023-11-24 18:04:47.460 [WRN] NO DATA, PENDING...
2023-11-24 18:04:50.632 [WRN] NO DATA, PENDING...
2023-11-24 18:04:54.243 [WRN] NO DATA, PENDING...
2023-11-24 18:04:57.350 [WRN] NO DATA, PENDING...
2023-11-24 18:05:00.418 [WRN] NO DATA, PENDING...
2023-11-24 18:05:03.725 [WRN] NO DATA, PENDING...
2023-11-24 18:05:06.825 [WRN] NO DATA, PENDING...

2023-11-24 18:05:07.156 [INF] DomainExService Sleep(ms):20000
2023-11-24 18:05:07.156 [INF] DomainExService End:0.01
2023-11-24 18:05:09.870 [WRN] NO DATA, PENDING...
2023-11-24 18:05:12.996 [WRN] NO DATA, PENDING...
2023-11-24 18:05:16.385 [WRN] NO DATA, PENDING...
2023-11-24 18:05:19.616 [WRN] NO DATA, PENDING...
2023-11-24 18:05:22.637 [WRN] NO DATA, PENDING...
2023-11-24 18:05:25.718 [WRN] NO DATA, PENDING...

2023-11-24 18:05:27.171 [INF] DomainExService Sleep(ms):20000
2023-11-24 18:05:27.171 [INF] DomainExService End:0.01
2023-11-24 18:05:29.258 [WRN] NO DATA, PENDING...
2023-11-24 18:05:32.278 [WRN] NO DATA, PENDING...
2023-11-24 18:05:35.369 [WRN] NO DATA, PENDING...
2023-11-24 18:05:38.402 [WRN] NO DATA, PENDING...
2023-11-24 18:05:41.880 [WRN] NO DATA, PENDING...
2023-11-24 18:05:45.660 [WRN] NO DATA, PENDING...

2023-11-24 18:05:47.216 [INF] DomainExService Sleep(ms):20000
2023-11-24 18:05:47.216 [INF] DomainExService End:0.01
2023-11-24 18:05:48.671 [WRN] NO DATA, PENDING...
2023-11-24 18:05:51.913 [WRN] NO DATA, PENDING...
```

Hello World!

Hello world!

OK

Operation: ● Inject DLL ○ Free DLL

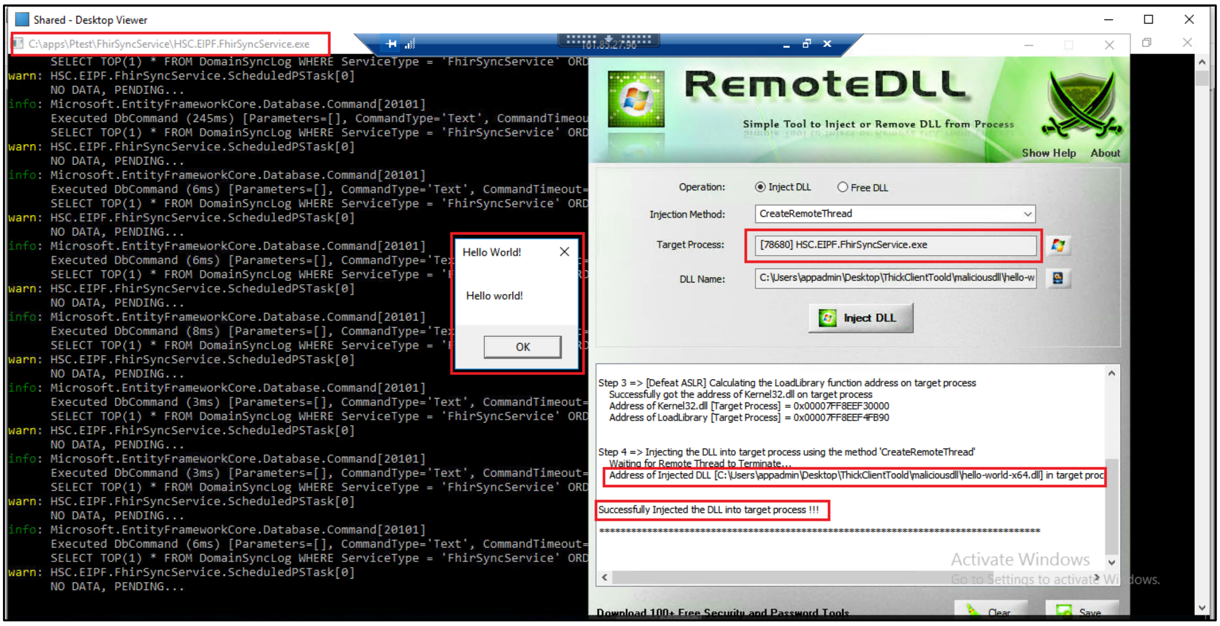
Injection Method: CreateRemoteThread

Target Process: [124644] HSC.EIPF.DomainMappingSyncService.exe

DLL Name: C:\Users\appadmin\Desktop\ThickClientToold\maliciousdll\hello-w

```
Step 3 => [Defeat ASLR] Calculating the LoadLibrary function address on target process
   Successfully got the address of Kernel32.dll on target process
   Address of Kernel32.dll [Target Process] = 0x00007FF8EEF30000
   Address of LoadLibrary [Target Process] = 0x00007FF8EEF4FB90

Step 4 => Injecting the DLL into target process using the method 'CreateRemoteThread'
   Waiting for Remote Thread to Terminate...
   Address of Injected DLL [C:\Users\appadmin\Desktop\ThickClientToold\maliciousdll\hello-world-x64.dll] in target proc

Successfully Injected the DLL into target process !!!
************************************************************************************
```

HSC.EIPF.DomainMappingSyncService.exe


Shared - Desktop Viewer
RemoteDLL
Simple Tool to Inject or Remove DLL from Process
Show Help
About
Inject DLL
Download 100+ Free Security and Password Tools
Clear
Save
Activate Windows
Go to Settings to activate Windows.

C:\apps\Ptest\FhirSyncService\HSC.EIPF.FhirSyncService.exe

```
     SELECT TOP(1) * FROM DomainSyncLog WHERE ServiceType = 'FhirSyncService' ORD
warn: HSC.EIPF.FhirSyncService.ScheduledPSTask[0]
      NO DATA, PENDING...
info: Microsoft.EntityFrameworkCore.Database.Command[20101]
      Executed DbCommand (245ms) [Parameters=[], CommandType='Text', CommandTimeou
      SELECT TOP(1) * FROM DomainSyncLog WHERE ServiceType = 'FhirSyncService' ORD
warn: HSC.EIPF.FhirSyncService.ScheduledPSTask[0]
      NO DATA, PENDING...
info: Microsoft.EntityFrameworkCore.Database.Command[20101]
      Executed DbCommand (6ms) [Parameters=[], CommandType='Text', CommandTimeout=
      SELECT TOP(1) * FROM DomainSyncLog WHERE ServiceType = 'FhirSyncService' ORD
warn: HSC.EIPF.FhirSyncService.ScheduledPSTask[0]
      NO DATA, PENDING...
info: Microsoft.EntityFrameworkCore.Database.Command[20101]
      Executed DbCommand (6ms) [Parameters=[], CommandType='Tex
      SELECT TOP(1) * FROM DomainSyncLog WHERE ServiceType = 'F
warn: HSC.EIPF.FhirSyncService.ScheduledPSTask[0]
      NO DATA, PENDING...
info: Microsoft.EntityFrameworkCore.Database.Command[20101]
      Executed DbCommand (8ms) [Parameters=[], CommandType='Tex
      SELECT TOP(1) * FROM DomainSyncLog WHERE ServiceType = 'F
warn: HSC.EIPF.FhirSyncService.ScheduledPSTask[0]
      NO DATA, PENDING...
info: Microsoft.EntityFrameworkCore.Database.Command[20101]
      Executed DbCommand (3ms) [Parameters=[], CommandType='Text', CommandTimeout=
      SELECT TOP(1) * FROM DomainSyncLog WHERE ServiceType = 'FhirSyncService' ORD
warn: HSC.EIPF.FhirSyncService.ScheduledPSTask[0]
      NO DATA, PENDING...
info: Microsoft.EntityFrameworkCore.Database.Command[20101]
      Executed DbCommand (3ms) [Parameters=[], CommandType='Text', CommandTimeout=
      SELECT TOP(1) * FROM DomainSyncLog WHERE ServiceType = 'FhirSyncService' ORD
warn: HSC.EIPF.FhirSyncService.ScheduledPSTask[0]
      NO DATA, PENDING...
info: Microsoft.EntityFrameworkCore.Database.Command[20101]
      Executed DbCommand (6ms) [Parameters=[], CommandType='Text', CommandTimeout=
      SELECT TOP(1) * FROM DomainSyncLog WHERE ServiceType = 'FhirSyncService' ORD
warn: HSC.EIPF.FhirSyncService.ScheduledPSTask[0]
      NO DATA, PENDING...
```

Hello World!

Hello world!

OK

Operation: ● Inject DLL ○ Free DLL

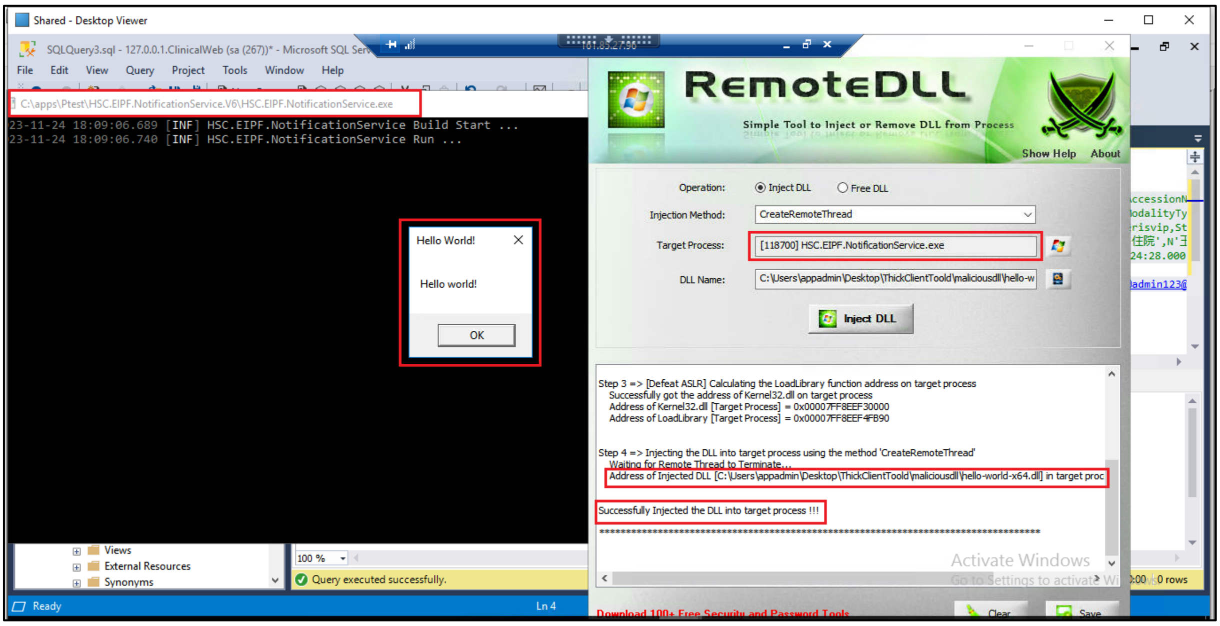
Injection Method: CreateRemoteThread

Target Process: [78680] HSC.EIPF.FhirSyncService.exe

DLL Name: C:\Users\appadmin\Desktop\ThickClientToold\maliciousdll\hello-w

```
Step 3 => [Defeat ASLR] Calculating the LoadLibrary function address on target process
   Successfully got the address of Kernel32.dll on target process
   Address of Kernel32.dll [Target Process] = 0x00007FF8EEF30000
   Address of LoadLibrary [Target Process] = 0x00007FF8EEF4FB90

Step 4 => Injecting the DLL into target process using the method 'CreateRemoteThread'
   Waiting for Remote Thread to Terminate...
   Address of Injected DLL [C:\Users\appadmin\Desktop\ThickClientToold\maliciousdll\hello-world-x64.dll] in target proc

Successfully Injected the DLL into target process !!!
****************************************************************************************
```

HSC.EIPF.FhirSyncService.exe


Shared - Desktop Viewer
SQLQuery3.sql - 127.0.0.1.ClinicalWeb (sa (267))* - Microsoft SQL Serv
File
Edit
View
Query
Project
Tools
Window
Help
Views
External Resources
Synonyms
100 %
Ready
Ln 4
0 rows
RemoteDLL
Simple Tool to Inject or Remove DLL from Process
Show Help
About
Inject DLL
Download 100+ Free Security and Password Tools
Clear
Save
Activate Windows
Go to Settings to activate Windows.

C:\apps\Ptest\HSC.EIPF.NotificationService.V6\HSC.EIPF.NotificationService.exe

```
23-11-24 18:09:06.689 [INF] HSC.EIPF.NotificationService Build Start ...
23-11-24 18:09:06.740 [INF] HSC.EIPF.NotificationService Run ...
```

Hello World!

Hello world!

OK

Query executed successfully.

Operation: ● Inject DLL ○ Free DLL

Injection Method: CreateRemoteThread

Target Process: [118700] HSC.EIPF.NotificationService.exe

DLL Name: C:\Users\appadmin\Desktop\ThickClientToold\maliciousdll\hello-w

```
Step 3 => [Defeat ASLR] Calculating the LoadLibrary function address on target process
   Successfully got the address of Kernel32.dll on target process
   Address of Kernel32.dll [Target Process] = 0x00007FF8EEF30000
   Address of LoadLibrary [Target Process] = 0x00007FF8EEF4FB90

Step 4 => Injecting the DLL into target process using the method 'CreateRemoteThread'
   Waiting for Remote Thread to Terminate...
   Address of Injected DLL [C:\Users\appadmin\Desktop\ThickClientToold\maliciousdll\hello-world-x64.dll] in target proc

Successfully Injected the DLL into target process !!!
****************************************************************************************
```

HSC.EIPF.NotificationService.exe

7.13 WindowsServices: Insecure Windows Service Permissions

Vulnerability Title	Insecure Windows Service Permissions
Vulnerability Category	Others
Severity	**Low**
CVSS V3 Calculation	CVSS Base Score: 3.4 CVSS:3.1/AV:P/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:N
Description	**Vulnerability Description:** During the security assessment, it was observed that At least one improperly configured Windows service may have a privilege escalation vulnerability. At least one Windows service executable with insecure permissions was detected on the remote host. Services configured to use an executable with weak permissions are vulnerable to privilege escalation attacks. This plugin checks if any of the following groups have permissions to modify executable files that are started by Windows services : - Everyone - Users - Domain Users - Authenticated Users **-** IIS Users have Write Permissions. **Exploitability Rational:** The attacker can exploit this by physical access to the machine. **Impact Rational:** An unprivileged user could modify or overwrite the executable with arbitrary code, which would be executed the next time the service is started. Depending on the user that the service runs as, this could result in privilege escalation.
Affected Systems/IP Address/URL	HSC.EIPF.DomainMappingSyncService.exe HSC.EIPF.FhirSyncService.exe

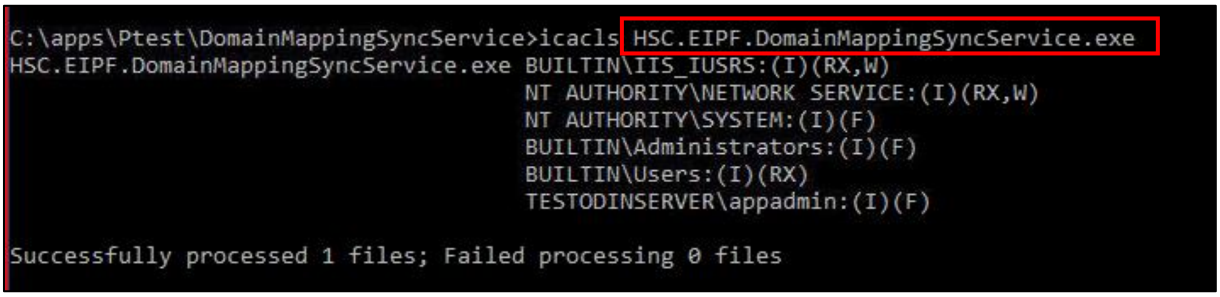
	HSC.EIPF.NotificationService.exe
Recommendation	Ensure the groups listed above (Everyone, Users, Domain Users & Authenticated Users) do not have permissions to modify or write service executables. Additionally, ensure these groups do not have Full Control permission to any directories that contain service executables.
Status	**Open**

Steps to Reproduce

Step 1: Run icacls <.exe>

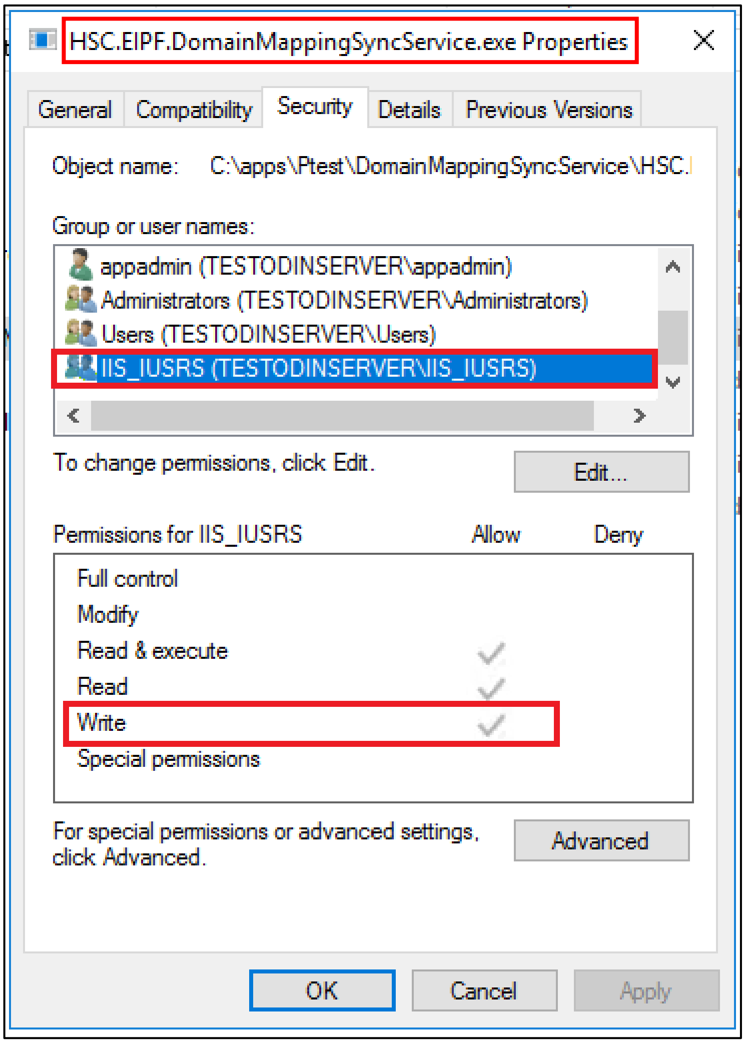
Step 2: Observe IIS_IUSRS have Write permissions.

Supportive Evidence:



```
C:\apps\Ptest\DomainMappingSyncService>icacls HSC.EIPF.DomainMappingSyncService.exe
HSC.EIPF.DomainMappingSyncService.exe BUILTIN\IIS_IUSRS:(I)(RX,W)
                                      NT AUTHORITY\NETWORK SERVICE:(I)(RX,W)
                                      NT AUTHORITY\SYSTEM:(I)(F)
                                      BUILTIN\Administrators:(I)(F)
                                      BUILTIN\Users:(I)(RX)
                                      TESTODINSERVER\appadmin:(I)(F)

Successfully processed 1 files; Failed processing 0 files
```

HSC.EIPF.DomainMappingSyncService.exe



HSC.EIPF.DomainMappingSyncService.exe Properties

Object name: C:\apps\Ptest\DomainMappingSyncService\HSC.I

Group or user names:

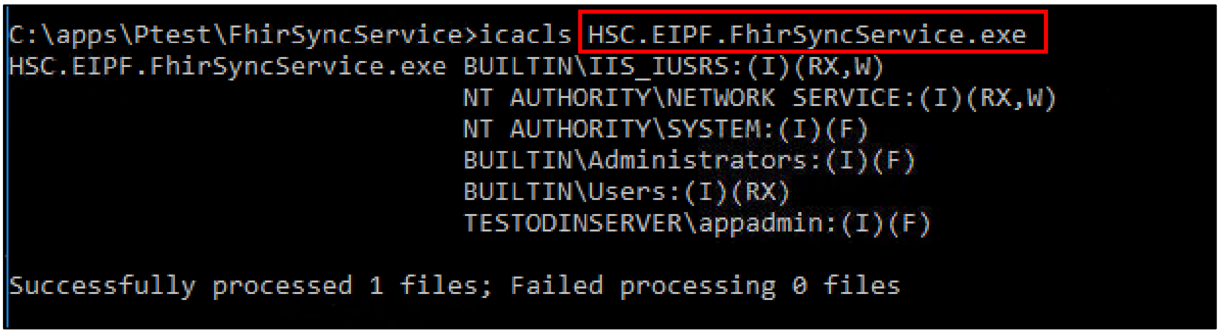
- appadmin (TESTODINSERVER\appadmin)
- Administrators (TESTODINSERVER\Administrators)
- Users (TESTODINSERVER\Users)
- IIS_IUSRS (TESTODINSERVER\IIS_IUSRS)

To change permissions, click Edit.

Permissions for IIS_IUSRS	Allow	Deny
Full control		
Modify		
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

HSC.EIPF.DomainMappingSyncService.exe

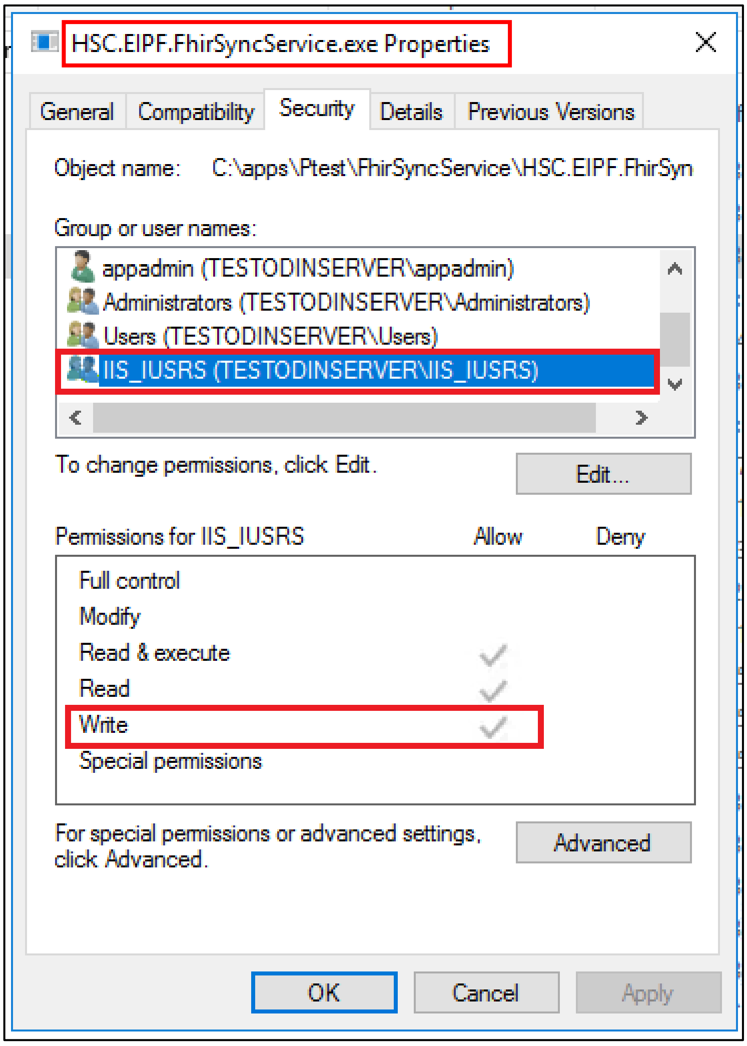


```
C:\apps\Ptest\FhirSyncService>icacls HSC.EIPF.FhirSyncService.exe
HSC.EIPF.FhirSyncService.exe BUILTIN\IIS_IUSRS:(I)(RX,W)
                             NT AUTHORITY\NETWORK SERVICE:(I)(RX,W)
                             NT AUTHORITY\SYSTEM:(I)(F)
                             BUILTIN\Administrators:(I)(F)
                             BUILTIN\Users:(I)(RX)
                             TESTODINSERVER\appadmin:(I)(F)

Successfully processed 1 files; Failed processing 0 files
```

HSC.EIPF.FhirSyncService.exe

This document is proprietary and confidential. No part of this document may be disclosed in any manner to a third party without the prior written consent of Philips Product Security and Services Office (PSSO).

Printed copies are uncontrolled unless authenticated.



HSC.EIPF.FhirSyncService.exe Properties

Object name: C:\apps\Ptest\FhirSyncService\HSC.EIPF.FhirSyn

Group or user names:

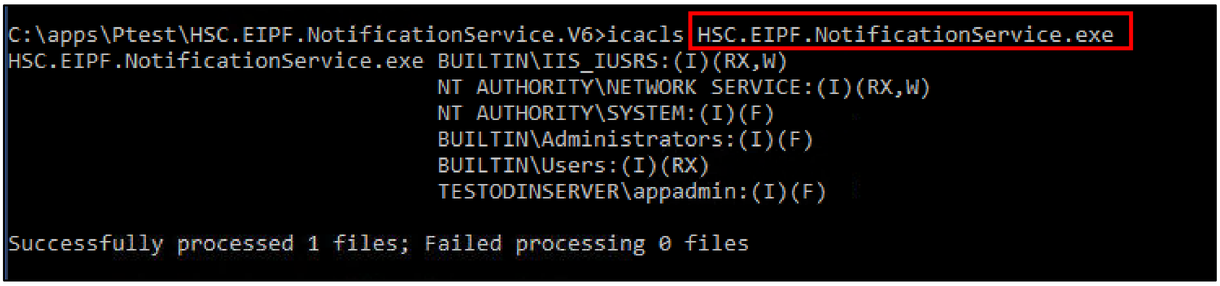
- appadmin (TESTODINSERVER\appadmin)
- Administrators (TESTODINSERVER\Administrators)
- Users (TESTODINSERVER\Users)
- IIS_IUSRS (TESTODINSERVER\IIS_IUSRS)

To change permissions, click Edit.

Permissions for IIS_IUSRS	Allow	Deny
Full control		
Modify		
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

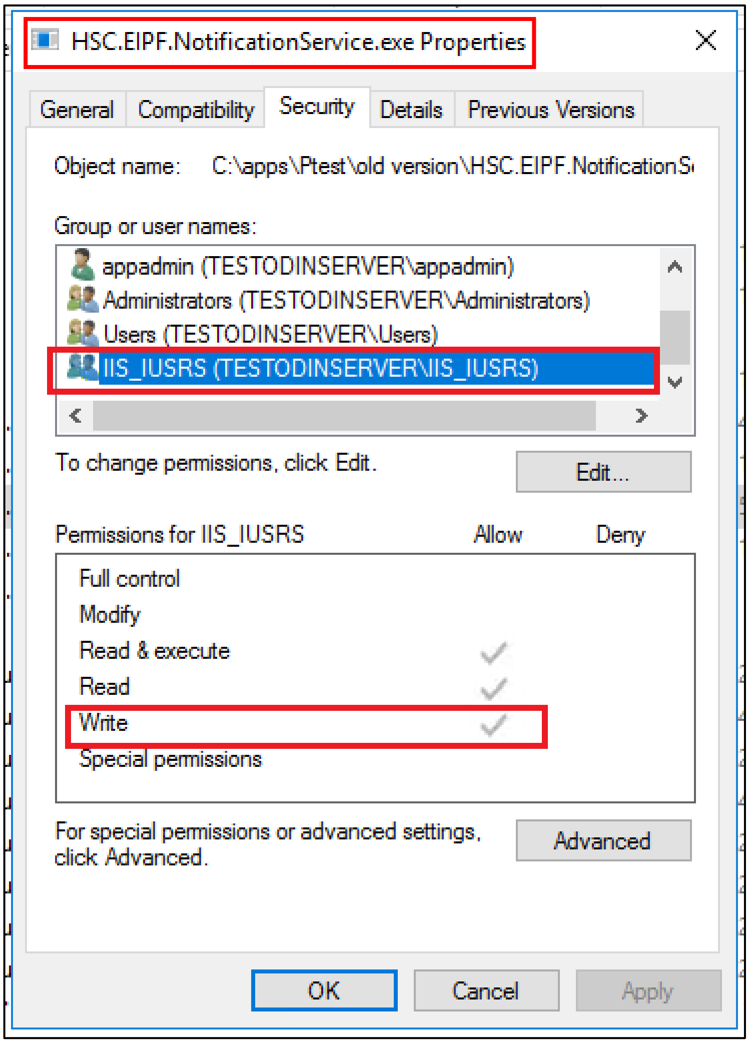
For special permissions or advanced settings, click Advanced.

HSC.EIPF.FhirSyncService.exe



```
C:\apps\Ptest\HSC.EIPF.NotificationService.V6>icacls HSC.EIPF.NotificationService.exe
HSC.EIPF.NotificationService.exe BUILTIN\IIS_IUSRS:(I)(RX,W)
                                 NT AUTHORITY\NETWORK SERVICE:(I)(RX,W)
                                 NT AUTHORITY\SYSTEM:(I)(F)
                                 BUILTIN\Administrators:(I)(F)
                                 BUILTIN\Users:(I)(RX)
                                 TESTODINSERVER\appadmin:(I)(F)

Successfully processed 1 files; Failed processing 0 files
```

HSC.EIPF.NotificationService.exe



HSC.EIPF.NotificationService.exe Properties

Object name: C:\apps\Ptest\old version\HSC.EIPF.NotificationS

Group or user names:

- appadmin (TESTODINSERVER\appadmin)
- Administrators (TESTODINSERVER\Administrators)
- Users (TESTODINSERVER\Users)
- IIS_IUSRS (TESTODINSERVER\IIS_IUSRS)

To change permissions, click Edit.

Permissions for IIS_IUSRS	Allow	Deny
Full control		
Modify		
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

HSC.EIPF.NotificationService.exe

8. Tools Used

Scope	Tools Used
Web Services	Burpsuite pro, Postman, Nmap
Windows Services	Remote DLL, Sigcheck, icacls, Process Hacker 2, Procmon

9. Automated Tool Report

nmap.txt

HSC.EIPF.FhirSyncService.txt

10. Manual Test Reports and Test Case Execution

2844_EIPF-1.1.0_TestSuites.xlsx